LUIS RIBES • PAVEL ZALESSKII

Volume 40

Ergebnisse der Mathematik und ihrer Grenzgebiete
3. Folge

A Series of Modern Surveys in Mathematics

Profinite Groups

Second Edition

Springer

Ergebnisse der Mathematik und ihrer Grenzgebiete

Volume 40

3. Folge

A Series of Modern Surveys in Mathematics

Luis Ribes • Pavel Zalesskii

Profinite Groups

Second edition

Springer

Luis Ribes
Dept. Mathematics & Statistics
Carleton University
Ottawa, ON K1S 5B6
Canada
lribes@math.carleton.ca

Pavel Zalesskii
Depto. Matemática
Universidade de Brasília
Brasilia, DF
Brazil
pz@mat.unb.br

ISBN 978-3-642-01641-7 e-ISBN 978-3-642-01642-4
DOI 10.1007/978-3-642-01642-4
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2010921917

Mathematics Subject Classification (2000): 12G05, 20E05, 20E06, 20E18, 20J05

Cover design: VTEX, Vilnius

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Para Marisa, Alfonso y David

Людмиле и Алику

Preface to the Second Edition

This new edition contains a few additions. The main ones are three new Appendices. Appendix B contains a new characterization of free pro-$\mathcal{C}$ groups, based on work of D. Harbater and K. Stevenson. Appendix C, based on a paper of A. Lubotzky, establishes the basic facts about presentations of finitely generated profinite groups in terms of generators and relators; it complements Section 7.8 where we consider presentations of pro-p groups. Appendix D contains a new self-contained and conceptually simpler approach to the proof of some classical subgroup theorems, like the Nielsen-Schreier and the Kurosh theorems, and some new ones; it is based on a paper of B. Steinberg and the first author.

In general we have maintained the original numeration, with only a couple of exceptions. We have inserted numerous additions throughout the text in the form of new results, better proofs, corrections, etc. We have also enlarged the bibliography. A few more open questions have been added; in the list of these open questions that we collect at the end of the book, we have noted those problems that have been solved after the first edition with comments and references. Theorem 3.5.13 gives a complete solution, due to J-P. Serre, of one of those previously open questions.

Several colleagues and friends have pointed out needed corrections or explanations and have made useful suggestions. We thank specially M. Aka, K. Auinger, G. Brumfiel, B. Deschamps, M. Jarden, D. Kochloukova and J-P. Serre.

March, 2009

Luis Ribes, Madrid
Pavel Zalesskii, Brasilia

Preface to the First Edition

The aim of this book is to serve both as an introduction to profinite groups and as a reference for specialists in some areas of the theory. In neither of these two aspects have we tried to be encyclopedic. After some necessary background, we thoroughly develop the basic properties of profinite groups and introduce the main tools of the subject in algebra, topology and homology. Later we concentrate on some topics that we present in detail, including recent developments in those areas.

Interest in profinite groups arose first in the study of the Galois groups of infinite Galois extensions of fields. Indeed, profinite groups are precisely Galois groups and many of the applications of profinite groups are related to number theory. Galois groups carry with them a natural topology, the Krull topology. Under this topology they are Hausdorff compact and totally disconnected topological groups; these properties characterize profinite groups. Another important fact about profinite groups is that they are determined by their finite images under continuous homomorphisms: a profinite group is the inverse limit of its finite images. This explains the connection with abstract groups. If G is an infinite abstract group, one is interested in deducing properties of G from corresponding properties of its finite homomorphic images. The kernels of all homomorphisms of G into finite groups form a fundamental system of neighborhoods for a topology on G, and completion of G with respect to this topology gives a profinite group. In the last decades there has been an extensive literature on profinite groups and one of the aims of this book is to present some of these important results.

The first comprehensive exposition of the theory of profinite groups appeared in the book 'Cohomologie Galoisienne' by J-P. Serre in 1964. Its emphasis is on cohomological properties and their applications to field theory and number theory. This deceptively slim volume contains a wealth of information, some of it not found elsewhere. We have learnt a great deal from Serre's book throughout the years and this, no doubt, is reflected in our exposition in the present book.

We describe briefly the contents of our book. The first three chapters deal with the basic tools and the main properties of profinite groups. In Chapter 1 we have collected information about inverse and direct limits and their algebraic and topological properties, which is used throughout the book. Chapter 2 contains a fairly detailed account of general profinite groups. The results are presented in the context of pro-$\mathcal{C}$ groups (inverse limits of groups in $\mathcal{C}$), where $\mathcal{C}$ is a convenient class of finite groups, which includes the classes of profinite and pro-p groups as particular cases. The minimum we require of such a class $\mathcal{C}$ is that it should be a 'formation' (i.e., closed under taking quotients and finite subdirect products); but often we assume that $\mathcal{C}$ is a 'variety' (i.e., closed under taking subgroups, quotients and finite direct products). Although this approach requires the reader to become familiar with a little more terminology (but not much more than what is indicated above), this is compensated by being able to bring many related concepts and results together. Sometimes we assume throughout a chapter or a section that $\mathcal{C}$ satisfies certain conditions; when that happens we indicate those assumptions in italics at the beginning of the chapter or section.

The main properties of free profinite (pro-$\mathcal{C}$) groups are developed in Chapter 3. These include several useful characterizations in terms of lifting maps à la Iwasawa and the study of the structure of open subgroups of free pro-$\mathcal{C}$ groups. Chapter 4 considers properties of particular profinite groups, including profinite abelian groups, Frobenius profinite groups and automorphism groups of finitely generated profinite groups.

Chapters 5–7 deal with homological aspects of profinite groups. In Chapter 5, we consider modules over profinite rings, particularly complete group rings, and constructions involving them. Chapter 6 establishes the fundamental results of homology and cohomology groups of profinite groups. Here we combine a computational approach with a conceptual one: on the one hand, we define homology and cohomology groups by means of standard resolutions, and on the other hand, we give a more abstract description, using the language of universal functors. Chapter 7 contains cohomological characterizations of projective profinite groups and the Tate characterization of free pro-p groups.

Chapter 8 considers closed normal subgroups of free profinite groups, and in particular, conditions under which such subgroups are free profinite. We also study similar properties for closed subnormal subgroups and accessible subgroups. This chapter includes Mel'nikov's theory of homogeneous groups, which gives a description of certain closed subgroups of free pro-$\mathcal{C}$ groups (other than pro-p).

Chapter 9 establishes the main properties of the basic 'free constructions' of profinite groups: free and amalgamated products and HNN-extensions. This is the beginning of the theory of profinite groups acting on 'profinite trees', which we shall develop in a subsequent book.

The last section of each chapter gives some of the history of the theory that has been developed, and indicates the names of the main contributors. These sections also include statements or references to results not treated in the main body of the chapters.

Throughout the text we have included a series of open questions that are also gathered at the end of book.

We thank Hendrik Lenstra Jr. for his suggestion that a book such as this should be written for the Ergebnisse Series. His contagious optimism and enthusiasm, and his interest in our ideas and projects have been very uplifting and helpful.

Several colleagues and friends have read parts of the book. We are specially grateful to Zoé Chatzidakis, Juan Ramón Delgado, John Dixon, Otto Kegel and Wolfgang Herfort for their comments and corrections; the errors and misprints that may remain are attributable entirely to us. We are greatly indebted to Jean-Pierre Serre for sharing with us some of his ideas and for his help in Section 6.9.

Part of this book was written while one of us (LR) was on sabbatical at the UNED in Madrid at the invitation of Emilio Bujalance. The congenial mathematical atmosphere that our colleagues have created there was very conducive to our work. It is a pleasure to thank them for wonderful discussions (mathematical and otherwise) and for their friendship. The advice of Javier Pérez regarding xy-pic was very useful and we thank him for the time he spent teaching us the tricks.

In the Summer of 1998 both authors participated in the program Research in Pairs of the Mathematisches Forschunginstitut in Oberwolfach while writing this book; we thank the Mathematisches Forschunginstitut for the use of the excellent Library there and for the opportunity to work together and uninterrupted in such quiet and confortable quarters in the beautiful and relaxing Schwarzwald.

The first author gratefully acknowledges the support of the National Science and Engineering Research Council of Canada and the Dirección General de Investigación y Desarrollo of Spain.

The second author thanks the Austrian Science Foundation and Fundação de Apoio à Pesquisa do Distrito Federal (Brazil) for support.

Responsibility for the writing of this book: L. Ribes has written most of the material in Chapters 1–8; the main exceptions are Section 4.5 and parts of Sections 4.4, 4.7, 5.6 and 8.3 which were written by P. Zalesskii; translation from Russian done by P. Zalesskii was important in the writing of Sections 8.5 and 8.10. Chapter 9 has been written by both authors. The editorial work for the final version of the book has been done by both authors.

January, 2000

Luis Ribes, Ottawa
Pavel Zalesskii, Brasilia

Table of Contents

Preface to the Second Edition vii

Preface to the First Edition ix

---

1 Inverse and Direct Limits
- 1.1 Inverse or Projective Limits 1
- 1.2 Direct or Inductive Limits 14
- 1.3 Notes, Comments and Further Reading 18

2 Profinite Groups
- 2.1 Pro-$\mathcal{C}$ Groups 19
- 2.2 Basic Properties of Pro-$\mathcal{C}$ Groups 28
  - Existence of Sections 29
  - Exactness of Inverse Limits of Profinite Groups 31
- 2.3 The Order of a Profinite Group and Sylow Subgroups 32
- 2.4 Generators 42
- 2.5 Finitely Generated Profinite Groups 44
- 2.6 Generators and Chains of Subgroups 47
- 2.7 Procyclic Groups 51
- 2.8 The Frattini Subgroup of a Profinite Group 52
- 2.9 Pontryagin Duality for Profinite Groups 58
- 2.10 Pullbacks and Pushouts 66
- 2.11 Profinite Groups as Galois Groups 68
- 2.12 Notes, Comments and Further Reading 72
  - Analytic Pro-p Groups 73
  - Number of Generators of a Group and of Its Profinite Completion 74

3 Free Profinite Groups
- 3.1 Profinite Topologies 75
- 3.2 The Pro-$\mathcal{C}$ Completion 78
  - The Completion Functor 81
- 3.3 Free Pro-$\mathcal{C}$ Groups 85
  - Free Pro-$\mathcal{C}$ Group on a Set Converging to 1 88

3.4 Maximal Pro-$\mathcal{C}$ Quotient Groups 96
3.5 Characterization of Free Pro-$\mathcal{C}$ Groups 98
3.6 Open Subgroups of Free Pro-$\mathcal{C}$ Groups 113
3.7 Notes, Comments and Further Reading 116
A Problem of Grothendieck on Completions 117

4 Some Special Profinite Groups
4.1 Powers of Elements with Exponents from $\widehat{\mathbf{Z}}$ 119
4.2 Subgroups of Finite Index in a Profinite Group 120
4.3 Profinite Abelian Groups 129
4.4 Automorphism Group of a Profinite Group 132
4.5 Automorphism Group of a Free Pro-p Group 137
4.6 Profinite Frobenius Groups 142
4.7 Torsion in the Profinite Completion of a Group 148
4.8 Notes, Comments and Further Reading 154
Profinite Torsion Groups 156
Normal Automorphisms 157

5 Discrete and Profinite Modules
5.1 Profinite Rings and Modules 159
Duality Between Discrete and Profinite Modules 165
5.2 Free Profinite Modules 166
5.3 G-modules and Complete Group Algebras 169
The Complete Group Algebra 170
5.4 Projective and Injective Modules 172
5.5 Complete Tensor Products 177
5.6 Profinite G-spaces 180
5.7 Free Profinite $[\![RG]\!]$-modules 189
5.8 Diagonal Actions 190
5.9 Notes, Comments and Further Reading 193
The Magnus Algebra and Free Pro-p Groups 193

6 Homology and Cohomology of Profinite Groups
6.1 Review of Homological Algebra 195
Right and Left Derived Functors 199
Bifunctors 200
The Ext Functors 201
The Tor Functors 202
6.2 Cohomology with Coefficients in $\mathbf{DMod}([\![RG]\!])$ 203
Standard Resolutions 205
The Inhomogeneous Bar Resolution 206
6.3 Homology with Coefficients in $\mathbf{PMod}([\![RG]\!])$ 208
6.4 Cohomology Groups with Coefficients in $\mathbf{DMod}(G)$ 212
6.5 The Functorial Behavior of $H^n(G,A)$ and $H_n(G,A)$ 214
The Inflation Map 215

6.6 $H^n(G, A)$ as Derived Functors on **DMod**(G) 220
6.7 Special Mappings 224
The Restriction Map in Cohomology 224
The Corestriction Map in Cohomology 225
The Corestriction Map in Homology 229
The Restriction Map in Homology 229
6.8 Homology and Cohomology Groups in Low Dimensions 231
$H^2(G, A)$ and Extensions of Profinite Groups 233
6.9 Extensions of Profinite Groups with Abelian Kernel 238
6.10 Induced and Coinduced Modules 242
6.11 The Induced Module $\mathrm{Ind}_H^G(B)$ for H Open 247
6.12 Notes, Comments and Further Reading 249

7 Cohomological Dimension
7.1 Basic Properties of Dimension 251
7.2 The Lyndon-Hochschild-Serre Spectral Sequence 256
7.3 Cohomological Dimension of Subgroups 261
7.4 Cohomological Dimension of Normal Subgroups and Quotients 266
7.5 Groups G with $cd_p(G) \leq 1$ 268
7.6 Projective Profinite Groups 271
7.7 Free Pro-p Groups and Cohomological Dimension 275
7.8 Generators and Relators for Pro-p Groups 278
7.9 Cup Products 282
7.10 Notes, Comments and Further Reading 288
Pro-p Groups G with one Defining Relator 290
Poincaré Groups 290

8 Normal Subgroups of Free Pro-$\mathcal{C}$ Groups
8.1 Normal Subgroup Generated by a Subset of a Basis 294
8.2 The S-rank 296
8.3 Accessible Subgroups 302
8.4 Accessible Subgroups H with $w_0(F/H) < \mathrm{rank}(F)$ 306
8.5 Homogeneous Pro-$\mathcal{C}$ Groups 313
8.6 Normal Subgroups 326
8.7 Proper Open Subgroups of Normal Subgroups 335
8.8 The Congruence Kernel of $\mathrm{SL}_2(\mathbf{Z})$ 340
8.9 Sufficient Conditions for Freeness 341
8.10 Characteristic Subgroups of Free Pro-$\mathcal{C}$ Groups 348
8.11 Notes, Comments and Further Reading 351

9 Free Constructions of Profinite Groups
9.1 Free Pro-$\mathcal{C}$ Products 353
9.2 Amalgamated Free Pro-$\mathcal{C}$ Products 367
9.3 Cohomological Characterizations of Amalgamated Products 374
9.4 Pro-$\mathcal{C}$ HNN-extensions 382
9.5 Notes, Comments and Further Reading 388

Open Questions 393

Appendix A: Spectral Sequences
A.1 Spectral Sequences 397
A.2 Positive Spectral Sequences 399
The Base Terms 400
The Fiber Terms 400
A.3 Spectral Sequence of a Filtered Complex 402
A.4 Spectral Sequences of a Double Complex 405
A.5 Notes, Comments and Further Reading 406

Appendix B: A Different Characterization of Free Profinite Groups
B.1 Free vs Projective Profinite Groups 407
B.2 Notes, Comments and Further Reading 408

Appendix C: Presentations of Profinite Groups
C.1 Presentations 409
C.2 Relation Modules 412
C.3 Notes, Comments and Further Reading 416

Appendix D: Wreath Products and Some Subgroup Theorems
D.1 Permutational Wreath Products 419
D.2 The Nielsen-Schreier Theorem for Free Pro-$\mathcal{C}$ Groups 423
D.3 The Kurosh Subgroup Theorem for Profinite Groups 425
Kurosh Systems 428
D.4 Subgroups of Projective Groups 432
D.5 Quasifree Profinite Groups 434
D.6 Notes, Comments and Further Reading 438

Bibliography 439

Index of Symbols 451

Index of Authors 455

Index of Terms 459

1 Inverse and Direct Limits

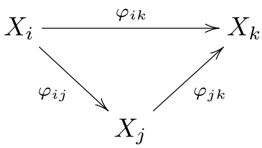
1.1 Inverse or Projective Limits

In this section we define the concept of inverse (or projective) limit and establish some of its elementary properties. Rather than developing the concept and establishing those properties under the most general conditions, we restrict ourselves to inverse limits of topological spaces or topological groups. We leave the reader the task of extending and translating the concepts and results obtained here to other objects such as sets, (topological) rings, modules, graphs..., or to more general categories.

Let $I = (I, \preceq)$ denote a *directed partially ordered set* or *directed poset*, that is, I is a set with a binary relation $\preceq$ satisfying the following conditions:

(a) $i \preceq i$, for $i \in I$;
(b) $i \preceq j$ and $j \preceq k$ imply $i \preceq k$, for $i, j, k \in I$;
(c) $i \preceq j$ and $j \preceq i$ imply $i = j$, for $i, j \in I$; and
(d) if $i, j \in I$, there exists some $k \in I$ such that $i, j \preceq k$.

An *inverse* or *projective system* of topological spaces (respectively, topological groups) over I, consists of a collection $\{X_i \mid i \in I\}$ of topological spaces (respectively, topological groups) indexed by I, and a collection of continuous mappings (respectively, continuous group homomorphisms) $\varphi_{ij} : X_i \longrightarrow X_j$, defined whenever $i \succeq j$, such that the diagrams of the form



commute whenever they are defined, i.e., whenever $i, j, k \in I$ and $i \succeq j \succeq k$. In addition we assume that φ_{ii} is the identity mapping id_{X_i} on X_i. We shall denote such a system by $\{X_i, \varphi_{ij}, I\}$, or by $\{X_i, \varphi_{ij}\}$ if the index set I is clearly understood. If X is a fixed topological space (respectively, topological group), we denote by $\{X, \mathrm{id}\}$ the inverse system $\{X_i, \varphi_{ij}, I\}$, where $X_i = X$ for all $i \in I$, and φ_{ij} is the identity mapping $\mathrm{id} : X \longrightarrow X$. We say that $\{X, \mathrm{id}\}$ is the *constant inverse system* on X.

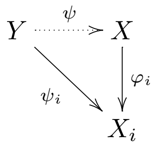
L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4_1,

Let Y be a topological space (respectively, topological group), $\{X_i, \varphi_{ij}, I\}$ an inverse system of topological spaces (respectively, topological groups) over a directed poset I, and let $\psi_i : Y \longrightarrow X_i$ be a continuous mapping (respectively, continuous group homomorphism) for each $i \in I$. These mappings ψ_i are said to be *compatible* if $\varphi_{ij}\psi_i = \psi_j$ whenever $j \preceq i$.

One says that a topological space (respectively, topological group) X together with compatible continuous mappings (respectively, continuous homomorphisms)

$$\varphi_i : X \longrightarrow X_i \quad (i \in I)$$

is an *inverse limit* or a *projective limit* of the inverse system $\{X_i, \varphi_{ij}, I\}$ if the following universal property is satisfied:



whenever Y is a topological space (respectively, topological group) and $\psi_i : Y \longrightarrow X_i$ $(i \in I)$ is a set of compatible continuous mappings (respectively, continuous homomorphisms), then there is a unique continuous mapping (respectively, continuous homomorphism) $\psi : Y \longrightarrow X$ such that $\varphi_i\psi = \psi_i$ for all $i \in I$. We say that ψ is "induced" or "determined" by the compatible homomorphisms ψ_i.

The maps $\varphi_i : X \longrightarrow X_i$ are called *projections*. The projection maps φ_i are not necessarily surjections. We denote the inverse limit by (X, φ_i), or often simply by X, by abuse of notation.

If $\{X_i, I\}$ is a collection of topological spaces (respectively, topological groups) indexed by a set I, its *direct product* or *cartesian product* is the topological space (respectively, topological group) $\prod_{i \in I} X_i$, endowed with the product topology. In the case of topological groups the group operation is defined coordinatewise.

Proposition 1.1.1 *Let $\{X_i, \varphi_{ij}, I\}$ be an inverse system of topological spaces (respectively, topological groups) over a directed poset I. Then*

(a) *There exists an inverse limit of the inverse system $\{X_i, \varphi_{ij}, I\}$;*
(b) *This limit is unique in the following sense. If (X, φ_i) and (Y, ψ_i) are two limits of the inverse system $\{X_i, \varphi_{ij}, I\}$, then there is a unique homeomorphism (respectively, topological isomorphism) $\varphi : X \longrightarrow Y$ such that $\psi_i\psi = \varphi_i$ for each $i \in I$.*

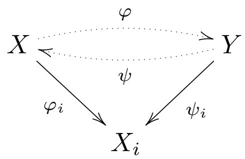
Proof. (a) Define X as the subspace (respectively, subgroup) of the direct product $\prod_{i \in I} X_i$ of topological spaces (respectively, topological groups) consisting of those tuples (x_i) that satisfy the condition $\varphi_{ij}(x_i) = x_j$ if $i \succeq j$.

Let

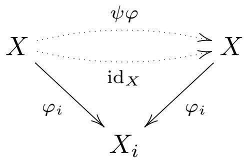
$$\varphi_i : X \longrightarrow X_i$$

denote the restriction of the canonical projection $\prod_{i\in I} X_i \longrightarrow X_i$. Then one easily checks that each φ_i is continuous (respectively, a continuous homomorphism), and that (X, φ_i) is an inverse limit.

(b) Suppose (X, φ_i) and (Y, ψ_i) are two inverse limits of the inverse system $\{X_i, \varphi_{ij}, I\}$.



Since the maps $\psi_i : Y \longrightarrow X_i$ are compatible, the universal property of the inverse limit (X, φ_i) shows that there exists a unique continuous mapping (respectively, continuous homomorphism) $\psi : Y \longrightarrow X$ such that $\varphi_i\psi = \psi_i$ for all $i \in I$. Similarly, since the maps $\varphi_i : X \longrightarrow X_i$ are compatible and (Y, ψ_i) is an inverse limit, there exists a unique continuous mapping (respectively, continuous homomorphism) $\varphi : X \longrightarrow Y$ such that $\psi_i\varphi = \varphi_i$ for all $i \in I$. Next observe that



commutes for each $i \in I$. Since, by definition, there is only one map satisfying this property, one has that $\psi\varphi = \mathrm{id}_X$. Similarly, $\varphi\psi = \mathrm{id}_Y$. Thus φ is a homeomorphism (respectively, topological isomorphism). □

If $\{X_i, \varphi_{ij}, I\}$ is an inverse system, we shall denote its inverse limit by $\varprojlim_{i\in I} X_i$, or $\varprojlim_{i} X_i$, or $\varprojlim_{I} X_i$, or $\varprojlim X_i$, depending on the context.

Lemma 1.1.2 *If $\{X_i, \varphi_{ij}\}$ is an inverse system of Hausdorff topological spaces* (*respectively, topological groups*), *then $\varprojlim X_i$ is a closed subspace* (*respectively, closed subgroup*) *of $\prod_{i\in I} X_i$.*

Proof. Let $(x_i) \in \left(\prod X_i\right) - \left(\varprojlim X_i\right)$. Then there exist $r, s \in I$ with $r \succeq s$ and $\varphi_{rs}(x_r) \neq x_s$. Choose open disjoint neighborhoods U and V of $\varphi_{rs}(x_r)$ and x_s in X_s, respectively. Let U' be an open neighborhood of x_r in X_r, such that $\varphi_{rs}(U') \subseteq U$. Consider the basic open subset $W = \prod_{i\in I} V_i$ of $\prod_{i\in I} X_i$ where $V_r = U'$, $V_s = V$ and $U_i = X_i$ for $i \neq r, s$. Then W is a open neighborhood of (x_i) in $\prod_{i\in I} X_i$, disjoint from $\varprojlim X_i$. This shows that $\varprojlim X_i$ is closed. □

A topological space is *totally disconnected* if every point in the space is its own connected component. For example, a space with the discrete topology is totally disconnected, and so is the rational line. It is easily checked that the direct product of totally disconnected spaces is totally disconnected. The following result is an immediate consequence of Tychonoff's theorem, that asserts that the direct product of compact spaces is compact (cf. Bourbaki [1989], Ch. 1, Theorem 3), and the fact that a closed subset of a compact space is compact.

Proposition 1.1.3 *Let* $\{X_i, \varphi_{ij}, I\}$ *be an inverse system of compact Hausdorff totally disconnected topological spaces* (*respectively, topological groups*) *over the directed set* I*. Then*

$$\varprojlim_{i \in I} X_i$$

is also a compact Hausdorff totally disconnected topological space (*respectively, topological group*)*.*

Proposition 1.1.4 *Let* $\{X_i, \varphi_{ij}\}$ *be an inverse system of compact Hausdorff nonempty topological spaces* X_i *over the directed set* I*. Then*

$$\varprojlim_{i \in I} X_i$$

is nonempty. In particular, the inverse limit of an inverse system of nonempty finite sets is nonempty.

Proof. For each $j \in I$, define a subset Y_j of $\prod X_i$ to consist of those (x_i) with the property $\varphi_{jk}(x_j) = x_k$ whenever $k \preceq j$. Using the axiom of choice and an argument similar to the one used in Lemma 1.1.2, one easily checks that each Y_j is a nonempty closed subset of $\prod X_i$. Observe that if $j \preceq j'$, then $Y_j \supseteq Y_{j'}$; it follows that the collection of subsets $\{Y_j \mid j \in I\}$ has the finite intersection property (i.e., any intersection of finitely many Y_j is nonempty), since the poset I is directed. Then, one deduces from the compactness of $\prod X_i$ that $\bigcap Y_j$ is nonempty. Since

$$\varprojlim_{i \in I} X_i = \bigcap_{j \in I} Y_j,$$

the result follows. □

Let $\{X_i, \varphi_{ij}, I\}$ and $\{X'_i, \varphi'_{ij}, I\}$ be inverse systems of topological spaces (respectively, topological groups) over the same directed poset I. A *map* or a *morphism* of inverse systems

$$\Theta : \{X_i, \varphi_{ij}\} \longrightarrow \{X'_i, \varphi'_{ij}\},$$

consists of a collection of continuous mappings (respectively, continuous homomorphisms) $\theta_i : X_i \longrightarrow X'_i$ $(i \in I)$ such that if $i \preceq j$, then the following diagram commutes

$$\begin{array}{ccc} X_j & \xrightarrow{\varphi_{ji}} & X_i \\ {\scriptstyle \theta_j}\downarrow & & \downarrow{\scriptstyle \theta_i} \\ X'_j & \xrightarrow{\varphi'_{ji}} & X'_i \end{array}$$

We say that the mappings θ_i are the *components* of Θ. A map

$$\Theta : \{X_i, \varphi_{ij}, I\} \longrightarrow \{X_i, \varphi_{ij}, I\}$$

of an inverse system to itself, whose components $\theta_i : X_i \longrightarrow X_i$ $(i \in I)$ are identity mappings, is called the identity map of the system $\{X_i, \varphi_{ij}, I\}$, and it is usually denoted by id. Composition of maps of inverse systems is defined in a natural way. That is, if

$$\Theta : \{X_i, \varphi_{ij}\} \longrightarrow \{X'_i, \varphi'_{ij}\},$$

with components θ_i, and

$$\Psi : \{X'_i, \varphi'_{ij}\} \longrightarrow \{X''_i, \varphi''_{ij}\},$$

with components ψ_i, are maps of inverse systems, then the components of the composition map

$$\Psi\Theta : \{X_i, \varphi_{ij}\} \longrightarrow \{X''_i, \varphi''_{ij}\},$$

are $\psi_i\theta_i$, $i \in I$. Thus one obtains a category of inverse systems of topological spaces (respectively, topological groups), whose objects are inverse systems of topological spaces (respectively, topological groups), and whose morphisms are maps of inverse systems.

Let $\{X_i, \varphi_{ij}\}$ and $\{X'_i, \varphi'_{ij}\}$ be inverse systems of topological spaces (respectively, topological groups) over the same directed poset I, and let $(X = \varprojlim X_i, \varphi_i)$ and $(X' = \varprojlim X'_i, \varphi'_i)$ be their corresponding inverse limits. Assume that

$$\Theta : \{X_i, \varphi_{ij}, I\} \longrightarrow \{X'_i, \varphi'_{ij}, I\}$$

is a map of inverse systems with components $\theta_i : X_i \longrightarrow X'_i$. Then the collection of compatible mappings

$$\theta_i\varphi_i : X \longrightarrow X'_i$$

induces a continuous mapping (respectively, continuous homomorphism)

$$\varprojlim \Theta = \varprojlim_{i \in I} \theta_i : \varprojlim_{i \in I} X_i \longrightarrow \varprojlim_{i \in I} X'_i.$$

Observe that $\varprojlim$ is a functor from the category of inverse systems of topological spaces (respectively,topological groups) over I to the category of topological spaces (respectively, topological groups); that is, $\varprojlim(\Psi\Theta) = \varprojlim \Psi \varprojlim \Theta$, and if id is the identity map on the inverse system $\{X_i, \varphi_{ij}, I\}$, then $\varprojlim \mathrm{id}$ is the identity map on the topological space (respectively, topological group) $\varprojlim_{i \in I} X_i$.

If the components $\theta_i : X_i \longrightarrow X'_i$ of a map $\Theta : \{X_i, \varphi_{ij}\} \longrightarrow \{X'_i, \varphi'_{ij}\}$ of inverse systems are embeddings, then obviously, so is

$$\varprojlim \theta_i : \varprojlim X_i \hookrightarrow \varprojlim X'_i.$$

In contrast, if each of the components θ_i is an onto mapping, $\varprojlim \theta_i$ is not necessarily onto. For example, consider the natural numbers $I = \mathbf{N}$, with the usual partial ordering, as our indexing poset; define two inverse systems (of discrete spaces) over I as follows: the constant inverse system $\{\mathbf{Z}, \mathrm{id}\}$, and the inverse system $\{\mathbf{Z}/p^n\mathbf{Z}, \varphi_{nm}\}$, where $\varphi_{nm} : \mathbf{Z}/p^n\mathbf{Z} \longrightarrow \mathbf{Z}/p^m\mathbf{Z}$ is the natural projection for $m \leq n$. For each $n \in \mathbf{N}$, define $\theta_n : \mathbf{Z} \longrightarrow \mathbf{Z}/p^n\mathbf{Z}$ to be the canonical epimorphism; then

$$\Theta = \{\theta_n\} : \{\mathbf{Z}, \mathrm{id}\} \longrightarrow \{\mathbf{Z}/p^n\mathbf{Z}, \varphi_{nm}\}$$

is a map of inverse systems. Observe that the inverse limit of the first system is $\mathbf{Z}$, while the inverse limit of the second can be identified with

$$\varprojlim \mathbf{Z}/p^n\mathbf{Z} = \{(x_n) \mid x_n \in \mathbf{Z}, x_n \equiv x_m \pmod{p^m} \text{ if } m \leq n\}.$$

The image of $\mathbf{Z}$ in $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$ under $\varprojlim \theta_n$ is the set of all constant tuples $\{(a_n) \mid a_n = t, t \in \mathbf{Z}\}$. On the other hand, the tuple (b_n), where $b_n = 1 + p + \cdots + p^{n-1}$, is in $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$, but it is not constant. Thus $\varprojlim \theta_n$ is not onto.

However, for inverse systems of compact Hausdorff spaces, one has the following result.

Lemma 1.1.5 *Let $\Theta : \{X_i, \varphi_{ij}, I\} \longrightarrow \{X'_i, \varphi'_{ij}, I\}$ be a map of inverse systems of compact Hausdorff topological spaces (respectively, topological groups), and assume that each component $\theta_i : X_i \longrightarrow X'_i$ $(i \in I)$ is onto. Then*

$$\varprojlim \Theta = \varprojlim_{i \in I} \theta_i : \varprojlim_{i \in I} X_i \longrightarrow \varprojlim_{i \in I} X'_i$$

is onto.

Proof. Let $(x'_i) \in \varprojlim X'_i$. Put $\widetilde{X}_i = \theta_i^{-1}(x'_i)$ $(i \in I)$. Since $\widetilde{X}_i$ is closed in the compact space X_i, it follows that $\widetilde{X}_i$ is compact $(i \in I)$. Observe that $\varphi_{ij}(\widetilde{X}_i) \subseteq \widetilde{X}_j$ for $i \succeq j$. Therefore, $\{\widetilde{X}_i, \varphi_{ij}\}$ is an inverse system of nonempty compact topological spaces (respectively, compact topological groups). By Proposition 1.1.4, $\varprojlim \widetilde{X}_i \neq \emptyset$. Let $(x_i) \in \varprojlim \widetilde{X}_i \subseteq \varprojlim X_i$. Then one has $(\varprojlim \Theta)(x_i) = (x'_i)$. □

Corollary 1.1.6 *Let $\{X_i, \varphi_{ij}, I\}$ be an inverse system of compact Hausdorff spaces and X a compact Hausdorff space. Suppose that $\{\varphi_i : X \longrightarrow X_i\}_{i\in I}$ is a set of compatible continuous surjective mappings. Then the corresponding induced mapping $\theta : X \longrightarrow \varprojlim X_i$ is onto.*

Proof. Consider the constant inverse system $\{X, \mathrm{id}\}$ over I. The collection $\{\theta_i\}_{i\in I}$ can be thought of as a map from $\{X, \mathrm{id}, I\}$ to $\{X_i, \varphi_{ij}, I\}$. Then $\theta = \varprojlim \theta_i$, and the result follows from the above proposition. □

Lemma 1.1.7 *Let $\{X_i, \varphi_{ij}, I\}$ be an inverse system of topological spaces over a directed set I, and let $\rho_i : X \longrightarrow X_i$ be compatible surjections from the space X onto the spaces X_i $(i \in I)$. Then either $\varprojlim X_i = \emptyset$ or the corresponding induced mapping $\rho : X \longrightarrow \varprojlim X_i$ maps X onto a dense subset of $\varprojlim X_i$.*

Proof. Suppose $\varprojlim X_i \neq \emptyset$. A general basic open subset V of $\varprojlim X_i$ can be described as follows: let $i_1, \dots, i_n$ be a finite subset of I and let U_{i_j} be an open subset of X_{i_j} $(j = 1, \dots, n)$; let

$$V = (\varprojlim X_i) \cap \left(\prod_{i\in I} V_i\right)$$

where $V_{i_j} = U_{i_j}$ $(j = 1, \dots, n)$ and $V_i = X_i$ for $i \neq i_1, \dots, i_n$. Assume such V is not empty. We have to show that $\rho(X) \cap V \neq \emptyset$. Let $i_0 \succeq i_1, \dots, i_n$, and let $y = (y_i) \in V$. Choose $x \in X$ so that $\rho_{i_0}(x) = y_{i_0}$. Then $\rho(x) \in V$. □

Corollary 1.1.8 *Let $\{X_i, \varphi_{ij}\}$ be an inverse system of compact Hausdorff spaces, $X = \varprojlim X_i$, and let $\varphi_i : X \longrightarrow X_i$ be the projections.*

(a) *If Y is a closed subspace of X, then $Y = \varprojlim \varphi_i(Y)$.*

(b) *If Y is a subspace of X, then*

$$\overline{Y} = \varprojlim \varphi_i(Y),$$

where $\overline{Y}$ is the closure of Y in X.

(c) *If Y and Y' are subspaces of X and $\varphi_i(Y) = \varphi_i(Y')$ for each i, then their closures in X coincide: $\overline{Y} = \overline{Y'}$.*

Proof. (a) Observe that there are obvious embeddings

$$Y \hookrightarrow \varprojlim \varphi_i(Y) \hookrightarrow \varprojlim X_i = X.$$

Moreover, by Corollary 1.1.6, the first of these embeddings is onto. Hence, $Y = \varprojlim \varphi_i(Y)$.

(b) According to Lemma 1.1.7, Y embeds as a dense subset of $\varprojlim \varphi_i(Y)$. Arguing as in Lemma 1.1.2 one sees that $\varprojlim \varphi_i(Y)$ is closed in X. Hence the result follows.

(c) This follows from (a) and (b). □

Let $(I, \preceq)$ be a directed poset. Assume that I' is a subset of I in such a way that $(I', \preceq)$ becomes a directed poset. We say that I' is *cofinal* in I if for every $i \in I$ there is some $i' \in I'$ such that $i \preceq i'$. If $\{X_i, \varphi_{ij}, I\}$ is an inverse system and I' is cofinal in I, then $\{X_i, \varphi_{ij}, I'\}$ becomes an inverse system in an obvious way, and we say that $\{X_i, \varphi_{ij}, I'\}$ is a *cofinal subsystem* of $\{X_i, \varphi_{ij}, I\}$.

Assume that $\{X_i, \varphi_{ij}, I'\}$ is a cofinal subsystem of $\{X_i, \varphi_{ij}, I\}$ and denote by $(\varprojlim_{i' \in I'} X_{i'}, \varphi'_{i'})$ and $(\varprojlim_{i \in I} X_i, \varphi_i)$ their corresponding inverse limits. For $j \in I$, let $j' \in I'$ be such that $j' \succeq j$. Define

$$\overline{\varphi}_j : \varprojlim_{I'} X_{i'} \longrightarrow X_j$$

as the composition of canonical mappings $\varphi_{j'j}\varphi'_{j'}$. Observe that the maps $\overline{\varphi}_j$ are well-defined (independent of the choice of j') and compatible. Hence they induce a map

$$\overline{\varphi} : \varprojlim_{I'} X_{i'} \longrightarrow \varprojlim_{I} X_i$$

such that $\varphi_j \overline{\varphi} = \overline{\varphi}_j$ $(j \in I)$. We claim that the mapping $\overline{\varphi}$ is a bijection. Note that if $(x_{i'}) \in \varprojlim_{i' \in I'} X_{i'}$ and $\overline{\varphi}(x_{i'}) = (y_i)$, then $y_{i'} = x_{i'}$ for $i' \in I'$. It follows that $\overline{\varphi}$ is an injection since I' is cofinal in I. To see that $\overline{\varphi}$ is a surjection, let $(y_i) \in \varprojlim_{i \in I} X_i$ and consider the element $(x_{i'})$, where $x_{i'} = y_{i'}$ for every $i' \in I'$. Then $(x_{i'}) \in \varprojlim_{i' \in I'} X_{i'}$ and clearly, $\overline{\varphi}(x_{i'}) = (y_i)$. This proves the claim. We record these results in the following lemma.

Lemma 1.1.9 *Let $\{X_i, \varphi_{ij}, I\}$ be a inverse system of compact topological spaces (respectively, compact topological groups) over a directed poset I and assume that I' is a cofinal subset of I. Then*

$$\varprojlim_{i \in I} X_i \cong \varprojlim_{i' \in I'} X_{i'}.$$

Proof. According to the above observations,

$$\overline{\varphi} : \varprojlim_{I'} X_{i'} \longrightarrow \varprojlim_{I} X_i$$

is a continuous bijection (respectively, group isomorphism). Since $\varprojlim_{i' \in I'} X_{i'}$ and $\varprojlim_{i \in I} X_i$ are compact spaces (respectively, compact topological groups), it follows that $\overline{\varphi}$ is a homeomorphism (respectively, topological isomorphism). We identify $\varprojlim_{i' \in I'} X_{i'}$ and $\varprojlim_{i \in I} X_i$ by means of this homeomorphism (respectively, topological isomorphism). □

An inverse system $\{X_i, \varphi_{ij}, I\}$ is called a *surjective inverse system* if each of the mappings φ_{ij} $(i \succeq j)$ is surjective. By Corollary 1.1.8(a), for any inverse system $\{X_i, \varphi_{ij}, I\}$, there is a corresponding surjective inverse system $\{\varphi_i(X), \varphi'_{ij}, I\}$ (where φ'_{ij} is just the restriction of φ_{ij} to $\varphi_i(X)$) with the same inverse limit X.

Let $\{X_i, \varphi_{ij}, I\}$ be an inverse system of topological spaces X_i over a poset I. Put $X = \varprojlim X_i$, and let $\varphi_j : X \longrightarrow X_j$ be the projection map. Assume that $X \neq \emptyset$. If φ_j is a surjection for each $i \in I$, then evidently $\varphi_{rs} : X_r \longrightarrow X_s$ is a surjection for all $r, s \in I$ with $r \succeq s$. The converse is not necessarily true. However, as the following proposition shows, the converse holds if one assumes in addition that each of the X_i is compact.

Proposition 1.1.10 *Let $\{X_i, \varphi_{ij}, I\}$ be a surjective inverse system of compact Hausdorff nonempty topological spaces X_i over a poset I. Then for each $j \in I$, the projection map $\varphi_j : \varprojlim X_i \longrightarrow X_j$ is a surjection.*

Proof. Fix $j \in I$. The set $I_j = \{i \in I \mid i \succeq j\}$ is cofinal in I; so, by Lemma 1.1.9, $\varprojlim_{i \in I_j} X_i \cong \varprojlim_{i \in I} X_i$. Therefore, we may assume that $i \succeq j$ for every $i \in I$. Let $x_j \in X_j$ and set $Y_r = \varphi_{rj}^{-1}(x_j)$ for $r \in I$. Since φ_{rj} is onto and continuous, Y_r is a nonempty compact subset of X_r $(r \in I)$. Furthermore, if $r \succeq s$ are indices in I, then $\varphi_{rs}(Y_r) \subseteq Y_s$. Hence $\{Y_r, \varphi_{rs}, I\}$ is an inverse system. According to Proposition 1.1.4, $\varprojlim Y_r \neq \emptyset$. Let $(y_r) \in \varprojlim Y_i \subseteq \varprojlim X_i$. Then $\varphi_j(y_r) = x_j$. □

In what follows we shall be specially interested in topological spaces X that arise as inverse limits

$$X = \varprojlim_{i \in I} X_i$$

of finite spaces X_i endowed with the discrete topology. We call such a space a *profinite space* or a *Boolean space*. Before we give some characterizations of profinite spaces, we need the following lemma.

Lemma 1.1.11 *Let X be a compact Hausdorff topological space and let $x \in X$. Then the connected component C of x is the intersection of all clopen (i.e., closed and open) neighborhoods of x.*

Proof. Let $\{U_t \mid t \in T\}$ be the family of all clopen neighborhoods of x, and put

$$A = \bigcap_{t \in T} U_t.$$

It is clear that every clopen neighborhood of x contains the connected component C of x; and so $C \subseteq A$. Therefore, it suffices to show that A is connected. Assume that $A = U \cup V$, $U \cap V = \emptyset$ with both U and V closed in A (and so, in X). We need to prove that either U or V is empty. Since X is Hausdorff and U and V are compact and disjoint, there exist open sets U' and V' in X such that $U' \supseteq U$, $V' \supseteq V$ and $U' \cap V' = \emptyset$. So,

$$[X - (U' \cup V')] \cap A = \emptyset.$$

Now, $X - (U' \cup V')$ is closed; hence, by the compactness of X, there exists a finite subfamily T' of T such that

$$[X - (U' \cup V')] \cap \left[\bigcap_{t' \in T'} U_{t'} \right] = \emptyset.$$

Observe that $B = \bigcap_{t' \in T'} U_{t'}$ is a clopen neighborhood of x, since T' is finite. On the other hand,

$$x \in (B \cap U') \cup (B \cap V') = B.$$

Say $x \in B \cap U'$. Plainly $B \cap U'$ is open, but it is also closed because $B \cap V'$ is open and $(X - B \cap V') \cap B = B \cap U'$. Therefore, $A \subseteq B \cap U' \subseteq U'$. Hence $A \cap V \subseteq A \cap V' = \emptyset$, and thus $V = \emptyset$. □

We say that an equivalence relation R on a topological space X is *open* (respectively, *closed*) if for every $x \in X$, the equivalence class xR of x is open (respectively, closed) in X. If R is open, then it is closed (xR is the complement of a union of open sets).

Observe that R is open in the above sense if and only if R considered as a subset of $X \times X$ is open. Indeed, assume that R is open, and let $(x, y) \in R$ ($x, y \in X$); then $xR \times yR$ is an open neighborhood of (x, y) contained in R, and hence R is an open subset of $X \times X$. Conversely, assume that R is an open subset of $X \times X$; since $(x, x) \in R$, there exists an open neighborhood U of x in X such that $U \times U \subseteq R$; hence $U \subseteq xR$, proving that xR is open in X, and thus that R is an open equivalence relation.

Theorem 1.1.12 *Let X be a topological space. Then the following conditions are equivalent.*

(a) *X is a profinite space*;
(b) *X is compact Hausdorff and totally disconnected*;
(c) *X is compact Hausdorff and admits a base of clopen sets for its topology.*

Proof. (a) ⇒ (b): Let X be a profinite space. Say $X = \varprojlim_{i \in I} X_i$, where each X_i is a finite space. By Proposition 1.1.3, X is compact Hausdorff and totally disconnected.

(b) ⇒ (c): Let X be a compact Hausdorff and totally disconnected space. Let W be an open neighborhood of a point x in X. We must show that W contains a clopen neighborhood of x. Let $\{U_t \mid t \in T\}$ be the family of all clopen neighborhoods of x. According to Lemma 1.1.11,

$$\{x\} = \bigcap_{t \in T} U_t.$$

Since $X - W$ is closed and disjoint from $\bigcap_{t\in T} U_t$, we deduce from the compactness of X that there is a finite subset T' of T such that

$$(X - W) \cap \left(\bigcap_{t\in T'} U_t \right) = \emptyset.$$

Thus $\bigcap_{t\in T'} U_t$ is a clopen neighborhood of x contained in W, as desired.

(c) $\Rightarrow$ (a): Suppose that X is compact Hausdorff and admits a base of clopen sets for its topology. Denote by $\mathcal{R}$ the collection of all open equivalence relations R on X; for such R, the space X/R is finite and discrete since X is compact. The set $\mathcal{R}$ is naturally ordered as follows: if $R, R' \in \mathcal{R}$, then $R \succeq R'$ if and only if $xR \subseteq xR'$ for all $x \in X$. Then $\mathcal{R}$ is a poset. To see that this poset is directed, let R_1 and R_2 be two equivalence relations on X. Define its intersection $R_1 \cap R_2$ to be the equivalence relation corresponding to the partition of X obtained by intersecting each equivalence class of R_1 with each equivalence class of R_2. Clearly $R_1 \cap R_2 \succeq R_1, R_2$. Now, if $R, R' \in \mathcal{R}$ and $R \succeq R'$, define $\varphi_{RR'} : X/R \longrightarrow X/R'$ by $\varphi_{RR'}(xR) = xR'$. Then $\{X/R, \varphi_{RR'}\}$ is an inverse system over $\mathcal{R}$. We shall show that

$$X \cong \varprojlim_{R\in\mathcal{R}} X/R.$$

Let

$$\psi : X \longrightarrow \varprojlim_{R\in\mathcal{R}} X/R$$

be the continuous mapping induced by the canonical continuous surjections

$$\psi_R : X \longrightarrow X/R.$$

By Corollary 1.1.6, ψ is a continuous surjection. To prove that ψ is a homeomorphism, it suffices then to prove that it is an injection, since X is compact. Let $x, y \in X$. By hypothesis, there exists a clopen neighborhood U of x that excludes y. Consider the equivalence relation R' on X with two equivalence classes: U and $X - U$. Clearly, $R' \in \mathcal{R}$ and $\psi_{R'}(x) \neq \psi_{R'}(y)$. So, $\psi(x) \neq \psi(y)$. Thus, ψ is an injection. $\square$

A topological space X is said to *satisfy the second axiom of countability* if it has a countable base of open sets; such space is also called *second countable* or *countably based*. A topological space X is said to *satisfy the first axiom of countability* if each point of X has a countable fundamental system of neighborhoods; such space is also called *first countable*.

Corollary 1.1.13 *A profinite space X is second countable if and only if*

$$X \cong \varprojlim{}_{i\in I} X_i,$$

where $(I, \preceq)$ is a countable totally ordered set and each X_i is a finite discrete space.

Proof. Suppose X is profinite and second countable. Consider the set $\mathcal{R}$ of all open equivalence relations on X. For $R \in \mathcal{R}$, xR is a finite union of basic open set. Hence $\mathcal{R}$ is countable. Say $\mathcal{R} = \{R_1, R_2, \dots\}$. For each natural number i, define $R'_i = R_1 \cap \cdots \cap R_i$. Then $R'_1 \preceq R'_2 \preceq \cdots$ and $\{R'_i \mid i \in \mathbf{N}\}$ is cofinal in $\mathcal{R}$. As seen in the proof of the implication (c) $\Rightarrow$ (a) in the theorem, $X = \varprojlim_{R \in \mathcal{R}} X/R$. Thus $X = \varprojlim_{i \in \mathbf{N}} X/R'_i$.

Conversely assume that $X = \varprojlim_{i \in I} X_i$, where the poset $(I, \preceq)$ is countable and each X_i is a finite discrete space. Then obviously $\prod_{i \in I} X_i$ is second countable and profinite; thus so is X. □

Exercise 1.1.14 Let $\{X_i \mid i \in I\}$ be a collection of spaces. Prove that

$$\prod_{i \in I} X_i$$

can be expressed as an inverse limit of direct products $\prod_{i \in F} X_i$, where F runs through the finite subsets of I.

Exercise 1.1.15 Let $\{X_i, \varphi_{ij}\}$ be an inverse system of topological spaces indexed by a poset I, $X = \varprojlim X_i$, and denote by $\varphi_i : X \longrightarrow X_i$ the projection map. Assume that for each $i \in I$, $\mathcal{U}_i$ is a base of open sets of X_i. Prove that $\{\varphi_i^{-1}(U) \mid U \in \mathcal{U}_i, i \in I\}$ is a base of open sets of X.

Lemma 1.1.16

(a) *Let $\{X_i, \varphi_{ij}, I\}$ be an inverse system of profinite spaces. Let*

$$X = \varprojlim_{i \in I} X_i$$

and denote by $\varphi_i : X \longrightarrow X_i$ the projection map $(i \in I)$. Let $\rho : X \longrightarrow Y$ be a continuous mapping onto a discrete finite space Y. Then ρ factors through some φ_k, that is, there exists some $k \in I$ and some continuous mapping $\rho' : X_k \longrightarrow Y$ such that $\rho = \rho' \varphi_k$.

(b) *Let $\{G_i, \varphi_{ij}, I\}$ be an inverse system of topological groups with underlying profinite spaces. Let*

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

and denote by $\varphi_i : G \longrightarrow G_i$ the projection continuous homomorphism $(i \in I)$. Let $\beta : G \longrightarrow H$ be a continuous homomorphism into a discrete finite group H. Then β factors through some φ_k, that is, there exists some $k \in I$ and some continuous homomorphism $\beta' : G_k \longrightarrow H$ such that $\beta = \beta' \varphi_k$.

Proof. (a) Assume first that each φ_i is a surjection. Let $Y = \{y_1, \dots, y_r\}$, and consider the clopen subsets $U_i = \rho^{-1}(y_i)$ $(i = 1, \dots, r)$ of X. Clearly $X = \bigcup_{i=1}^r U_i$, and $U_i \cap U_j = \emptyset$ if $i \neq j$. Fix i. For each $x \in U_i$ choose an index $k_x \in I$ and a clopen neighborhood $V_x = V_x^i$ of $\varphi_{k_x}(x)$ in X_{k_x} such that $\varphi_{k_x}^{-1}(V_x) \subseteq U_i$ (see Exercise 1.1.15). Put $W_x = \varphi_{k_x}^{-1}(V_x)$. By the compactness of U_i, there are finitely many points $x_1, \dots, x_{t_i}$ in U_i such that $U_i = W_{x_1} \cup \cdots \cup W_{x_{t_i}}$. Choose an index $k \in I$ such that $k \geq k_{x_1}, \dots, k_{x_{t_i}}$. Replacing V_{x_s} by $\varphi_{kk_{x_s}}^{-1}(V_{x_s})$ $(s = 1, \dots, t_i)$, we may assume that $k_{x_1} = \cdots = k_{x_{t_i}} = k$. Note that this k depends on i; however, since I is directed, we may assume that in fact k is valid for all $i = 1, \dots, r$. Hence we have constructed clopen subsets $V_1^i, \dots, V_{t_i}^i$ of X_k such that $U_i = \bigcup_{s=1}^{t_i} \varphi_k^{-1}(V_s^i)$ $(i = 1, \dots, r)$. Put $V^i = \bigcup_{s=1}^{t_i} V_s^i$. Then $V^i \cap V^j = \emptyset$ if $i \neq j$ $(1 \leq i, j \leq r)$; furthermore, $X_k = \bigcup_{i=1}^{r} V^i$ since φ_k is a surjection. Define $\rho' : X_k \longrightarrow Y$ by $\rho'(x) = y_i$ if $x \in V^i$. Then ρ' is a continuous mapping since the V^i are clopen and form a disjoint covering of X. Clearly $\rho = \rho' \varphi_k$.

To finish part (a), consider now the case when the projection maps φ_i are not necessarily surjective. By the construction above, there exists some $k \in I$ and a continuous surjection $\mu : \varphi_k(X) \longrightarrow Y$ such that $\rho = \mu\varphi_k$. Hence, it suffices to extend μ to a continuous map $\rho' : X_k \longrightarrow Y$. Put $Z = \varphi_k(X)$. For each $i = 1, \dots, r$, let $W_i = \mu^{-1}(y_i)$. Then $Z = W_1 \cup\!\!\!\cdot \cdots \cup\!\!\!\cdot\, W_r$ and each W_i is clopen in Z. Since X_k is a profinite space and Z is closed in X_k, there exist clopen subsets $W_1', \dots, W_r'$ of X_k such that $X_k = W_1' \cup\!\!\!\cdot \cdots \cup\!\!\!\cdot\, W_r'$ and $W_i = W_i' \cap Z$ $(i = 1, \dots, r)$. Define $\rho'(x) = y_i$ for $x \in W_i'$ $(i = 1, \dots, r)$. Then ρ' is clearly continuous and extends μ. This ends the proof of part (a).

(b) Thinking of G, H and each G_i as topological spaces, we infer from part (a) that β factors through a continuous function $\beta_{i_0} : G_{i_0} \longrightarrow H$, for some $i_0 \in I$. However β_{i_0} need not be a homomorphism. Put $I_0 = \{i \in I \mid i \succeq i_0\}$. For each $i \in I_0$, define $\beta_i : G_i \longrightarrow H$, by $\beta_i = \beta_{i_0}\varphi_{ii_0}$; then clearly $\beta = \beta_i\varphi_i$. We claim that for some $k \in I_0$, the map β_k is a homomorphism. To see this consider the continuous map

$$\eta : G \times G \longrightarrow H \times H, \qquad (g_1, g_2) \mapsto (\beta(g_1)\beta(g_2), \beta(g_1 g_2)),$$

and the analogous continuous maps $\eta_i : G_i \times G_i \longrightarrow H \times H$, for each $i \in I_0$, replacing β by β_i. It is easy to check that

$$G \times G = \varprojlim_{i \succeq i_0} G_i \times G_i, \qquad \eta = \varprojlim_{i \in I_0} \eta_i,$$

and

$$\eta(G \times G) = \varprojlim_{i \in I_0} \eta_i(G_i \times G_i) = \bigcap_{i \succeq i_0} \eta_i(G_i \times G_i).$$

Since $\eta_i(G_i \times G_i)$ is contained in the finite set $H \times H$ and since I_0 is a directed poset, it follows that

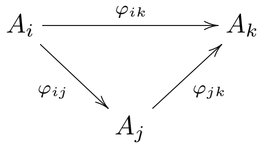
$$\eta(G \times G) = \eta_k(G_k \times G_k),$$

for some $k \in I_0$. Next observe that since β is a homomorphism, $\eta(G \times G) \subseteq \Delta = \{(h, h) \mid h \in H\}$. Therefore $\eta_k(G_k \times G_k) \subseteq \Delta$; thus η_k is a homomorphism. Put $\beta' = \eta_k$. $\square$

1.2 Direct or Inductive Limits

In this section we study direct (or inductive) systems and their limits. The definitions and some of the properties obtained here are found by dualizing the corresponding ones in the case of inverse (or projective) limits developed in Section 1.1; however there some specific results for direct limits that we want to emphasize. Again, we shall not try to develop the theory under the most general conditions; we are mainly interested in direct limits of abelian groups (or modules). So, to avoid unnecessary repetitions, we shall work within the category of abelian groups and leave the reader the task of translating the results for other categories (sets, rings, modules, graphs, etc.).

Let $I = (I, \preceq)$ be a partially ordered set (see Section 1.1) A *direct* or *inductive system* of abelian groups over I consists of a collection $\{A_i\}$ of abelian groups indexed by I and a collection of homomorphisms $\varphi_{ij} : A_i \longrightarrow A_j$, defined whenever $i \preceq j$, such that the diagrams of the form



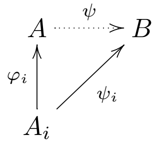
commute whenever $i \preceq j \preceq k$.

In addition, we assume that φ_{ii} is the identity mapping id_{A_i} on A_i. We shall denote such a system by $\{A_i, \varphi_{ij}, I\}$, or by $\{A_i, \varphi_{ij}\}$ if the index set I is clearly understood. If A is a fixed abelian group, we denote by $\{A, \mathrm{id}\}$ the direct system $\{A_i, \varphi_{ij}\}$, where $A_i = A$ for all $i \in I$, and φ_{ij} is the identity mapping $\mathrm{id} : A \longrightarrow A$. We say that $\{A, \mathrm{id}\}$ is the *constant direct system* on A.

Let A be an abelian group, $\{A_i, \varphi_{ij}, I\}$ a direct system of abelian groups over a directed poset I and assume that $\psi_i : A_i \longrightarrow A$ is a homomorphism for each $i \in I$. These mappings ψ_i are said to be *compatible* if $\psi_j \varphi_{ij} = \psi_i$ whenever $i \preceq j$. One says that an abelian group A together with compatible homomorphisms

$$\varphi_i : A_i \longrightarrow A$$

$(i \in I)$ is a *direct limit* or an *inductive limit* of the direct system $\{A_i, \varphi_{ij}, I\}$, if the following universal property is satisfied:



whenever B is an abelian group and $\psi_i : A_i \longrightarrow B$ $(i \in I)$ is a set of compatible homomorphisms, then there exists a unique homomorphism

$$\psi : A \longrightarrow B$$

such that $\psi\varphi_i = \psi_i$ for all $i \in I$. We say that ψ is "induced" or "determined" by the compatible homomorphisms ψ_i.

Proposition 1.2.1 *Let $\{A_i, \varphi_{ij}, I\}$ be a direct system of abelian groups over a directed poset I. Then there exists a direct limit of the system. Moreover, this limit is unique in the following sense: if (A, φ_i) and (A', φ'_i) are two limits, then there is a unique isomorphism $\eta : A \longrightarrow A'$ such that $\varphi'_i = \eta\varphi_i$ for each $i \in I$.*

Proof. The uniqueness is immediate. To show the existence of the direct limit of the system $\{A_i, \varphi_{ij}, I\}$, let U be the disjoint union of the groups A_i. Define a relation $\sim$ on U as follows: we say that $x \in A_i$ is equivalent to $y \in A_j$ if there exists $k \in I$ with $k \succeq i, j$ such that $\varphi_{ik}(x) = \varphi_{jk}(y)$. This is an equivalence relation. Denote by $\tilde{x}$ the equivalence class of $x \in A_i$ under this relation. Denote by A the set of all equivalence classes of U. Given $x \in A_i$ and $y \in A_j$ consider an index $k \in I$ with $k \succeq i, j$, and define $\tilde{x} + \tilde{y}$ to be the class of $\varphi_{ik}(x) + \varphi_{jk}(y)$; this is easily seen to be well-defined. Then A becomes an abelian group under this operation (its zero element is the class represented by the zero of A_i for any $i \in I$). For each $i \in I$, let $\varphi_i : A_i \longrightarrow A$ be given by $\varphi_i(x) = \tilde{x}$; then φ_i is a homomorphism. To check that (A, φ_i) is a direct limit of the direct system $\{A_i, \varphi_{ij}, I\}$, let $\psi_i : A_i \longrightarrow B$ $(i \in I)$ be a collection of compatible homomorphisms into an abelian group B. Define the induced homomorphism $\psi : A \longrightarrow B$ as follows. Let $a \in A$; say $a = \varphi_i(x)$ for some $x \in A_i$ and $i \in I$. Then define $\psi(a) = \psi_i(x)$. Observe that ψ is a well-defined homomorphism and $\psi\varphi_i = \psi_i$ for all $i \in I$. Furthermore, ψ is the only possible homomorphism satisfying these conditions. □

If $\{A_i, \varphi_{ij}, I\}$ is a direct system, we denote its direct limit by $\varinjlim_{i \in I} A_i$, or $\varinjlim_i A_i$, or $\varinjlim_I A_i$, or $\varinjlim A_i$, depending on the context.

Exercise 1.2.2 Let $\{A_i, \varphi_{ij}, I\}$ be a direct system of abelian groups over a directed poset I, and let I' be a cofinal subset of I. Show that the groups $\{A_i \mid i \in I'\}$ form in a natural way a direct system of abelian groups over I', and

$$\varinjlim_{i \in I} A_i = \varinjlim_{i \in I'} A_i.$$

The following exercise provides an alternative way of constructing direct limits; this procedure is the dual of the construction for inverse limits used in the proof of Proposition 1.1.1.

Exercise 1.2.3 Let $\{A_i, \varphi_{ij}, I\}$ be a direct system of abelian groups over a directed poset I. Define A to be the quotient group of the direct sum $\bigoplus_{i \in I} A_i$ modulo the subgroup R generated by the elements of the form $\varphi_{ij}(x) - x$ for all $x \in A_i$, $i \in I$ and $i \preceq j$. There are natural homomorphisms $\varphi_i : A_i \longrightarrow A$. Prove that A together with these homomorphisms is a direct limit of the system $\{A_i, \varphi_{ij}, I\}$.

Proposition 1.2.4 *Let $\{A_i, \varphi_{ij}\}$ be a direct system of abelian groups over a directed poset I, $A = \varinjlim A_i$ its direct limit and $\varphi_i : A_i \longrightarrow A$ the canonical homomorphisms. Then*

(a) $A = \bigcup_{i \in I} \varphi_i(A_i)$;
(b) *Let $x \in A_i$ and assume $\varphi_i(x) = 0$; then there exists some $k \succeq i$ such that $\varphi_{ik}(x) = 0$;*
(c) *If φ_{ik} is an injection for each $k \succeq i$, then φ_i is an injection;*
(d) *If φ_{ik} is onto for each $k \succeq i$, then φ_i is a surjection.*

Proof. Part (a) is obvious from our construction. To prove (b), note that $\varphi_i(x) = 0$ means that $\tilde{x} = \tilde{0}$, where $0 \in A_j$ for some $j \in I$ (we use the notation of the proof of Proposition 1.2.1). Therefore, there exists $k \succeq i, j$ such that $\varphi_{ik}(x) = \varphi_{jk}(0) = 0$. Part (c) follows from (b). To show (d), let $a \in A$; then, by construction, $a = \tilde{y}$, where $y \in A_j$ for some $j \in I$. Choose $k \succeq i, j$. Since φ_{ik} is onto, there exists $x \in A_i$ such that $\varphi_{ik}(x) = \varphi_{jk}(y)$; therefore $\varphi_i(x) = \tilde{x} = \tilde{y} = a$. □

Example 1.2.5

(1) The prototype of a direct limit is a union. If an abelian group A is a union $A = \bigcup_{i \in I} A_i$ of subgroups A_i, then A is the direct limit of the subgroup generated by the finite unions $\bigcup_{j \in J} A_j$, where J ranges over the finite subsets of I. Conversely, if
$$A = \varinjlim_{i \in I} A_i$$
is a direct limit of a direct system $\{A_i, \varphi_{ij}, I\}$, and if $\varphi_i : A_i \longrightarrow A$ are the canonical maps, then
$$A = \bigcup_{i \in I} \varphi_i(A_i).$$
(2) Every abelian group A is a direct limit of its finitely generated subgroups. In particular, if A is torsion, it is the direct limit of its finite subgroups.
(3) Let p be a prime number. We use the notation C_{p^∞} for the *p-quasicyclic* or Prüfer group, i.e., the group of p^nth complex roots of unity, with n running over all non-negative integers. Equivalently, C_{p^∞} can be defined as the direct limit
$$C_{p^\infty} = \varinjlim_{n} C_{p^n},$$
of the direct system of cyclic groups $\{C_{p^n}, \varphi_{nm}\}$, where the homomorphism $\varphi_{nm} : C_{p^n} \longrightarrow C_{p^m}$, defined for $n \leq m$, is the natural injection.

A map
$$\Psi : \{A_i, \varphi_{ij}, I\} \longrightarrow \{A'_i, \varphi'_{ij}, I\}$$

of direct systems $\{A_i, \varphi_{ij}, I\}$ and $\{A'_i, \varphi'_{ij}, I\}$ over the same directed poset I consists of a collection of homomorphisms

$$\psi_i : A_i \longrightarrow A'_i \quad (i \in I)$$

that commute with the canonical maps φ_{ij} and φ'_{ij}. That is, whenever $i \preceq j$, we have a commuting square

$$\begin{array}{ccc} A_i & \xrightarrow{\varphi_{ij}} & A_j \\ {\scriptstyle\psi_i}\downarrow & & \downarrow{\scriptstyle\psi_j} \\ A'_i & \xrightarrow[\varphi'_{ij}]{} & A'_j \end{array}$$

We refer to the homomorphisms ψ_{ij} as the *components* of the map Ψ.

Direct systems of abelian groups over a fixed poset I together with their maps, as defined above, form in a natural way a category. (This category is in fact an abelian category; although the analogous category of direct systems of sets, say, is not abelian.)

Let

$$\{A_i, \varphi_{ij}, I\} \quad \text{and} \quad \{A'_i, \varphi'_{ij}, I\}$$

be direct systems over the same poset $(I, \preceq)$, and let

$$A = \varinjlim A_i \quad \text{and} \quad A' = \varinjlim A'_i$$

be their corresponding direct limits, with canonical maps $\varphi_i : A_i \longrightarrow A$ and $\varphi'_i : A'_i \longrightarrow A'$, respectively. Associated with each map

$$\Psi = \{\psi_i\} : \{A_i, \varphi_{ij}, I\} \longrightarrow \{A'_i, \varphi'_{ij}, I\}$$

of direct systems, there is a homomorphism

$$\varinjlim \Psi = A \longrightarrow A'$$

defined by the universal property of direct limits:

$$\varinjlim \Psi = \varinjlim{}_{i \in I} \psi_i.$$

This is the unique homomorphism induced by the compatible maps

$$\varphi'_i \psi_i : A_i \longrightarrow A' \quad (i \in I).$$

With these definitions, it is straightforward to verify that $\varinjlim(\Psi\Psi') = \varinjlim(\Psi) \varinjlim(\Psi')$ and $\varinjlim(\mathrm{id}_{\{A_i, \varphi_{ij}, I\}}) = \mathrm{id}_{\varinjlim A_i}$; in other words, $\varinjlim$ is a functor from the category of direct systems of abelian groups over the same poset, to the category of abelian groups.

We restate all this as part of the following proposition.

Proposition 1.2.6 *Let I be a fixed poset. Then the collection $\mathfrak{D}$ of all direct systems of abelian groups over I and their maps form an abelian category. Furthermore, $\varinjlim$ is an exact* (*covariant*) *functor from $\mathfrak{D}$ to the category of abelian groups.*

The proof of this proposition follows easily from repeated applications of Proposition 1.2.4; we leave the details to the reader.

1.3 Notes, Comments and Further Reading

The material in this chapter is standard. For more details on inverse and direct limits the reader may consult, e.g., Eilenberg and Steenrod [1952], Bourbaki [1989] or Fuchs [1970].

2 Profinite Groups

2.1 Pro-$\mathcal{C}$ Groups

Let $\mathcal{C}$ be a nonempty class of finite groups [this will always mean that $\mathcal{C}$ contains all the isomorphic images of the groups in $\mathcal{C}$]. Define a *pro-$\mathcal{C}$ group* G as an inverse limit

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

of a surjective inverse system $\{G_i, \varphi_{ij}, I\}$ of groups G_i in $\mathcal{C}$, where each group G_i is assumed to have the discrete topology. We think of such a pro-$\mathcal{C}$ group G as a topological group, whose topology is inherited from the product topology on $\prod_{i\in I} G_i$.

The class $\mathcal{C}$ is said to be *subgroup closed* if whenever $G \in \mathcal{C}$ and $H \leq G$, then $H \in \mathcal{C}$. We remark that if the class $\mathcal{C}$ is subgroup closed, then any inverse limit of a (non-necessarily surjective) inverse system of groups in $\mathcal{C}$ is a pro-$\mathcal{C}$ group.

A group G is a *subdirect product* of a collection of groups $\{G_j \mid j \in J\}$ if there exists a collection of normal subgroups $\{N_j \mid j \in J\}$ of G such that $\bigcap_{j\in J} N_j = 1$ and $G/N_j \cong G_j$ for each $j \in J$. Observe that if G is a subdirect product of the groups $\{G_j \mid j \in J\}$, then G is isomorphic to a subgroup of the direct product $\prod_{i\in J} G_j$.

The properties of pro-$\mathcal{C}$ groups are obviously dependent on the type of class $\mathcal{C}$ that one considers. We are going to state a series of properties that a class $\mathcal{C}$ could satisfy which are of possible interest in this book. According to our needs, we shall assume that a class of finite groups $\mathcal{C}$ satisfies one or more of the following properties:

($\mathcal{C}$1) $\mathcal{C}$ is subgroup closed.
($\mathcal{C}$2) $\mathcal{C}$ is closed under taking quotients, that is, if $G \in \mathcal{C}$ and $K \triangleleft G$, then $G/K \in \mathcal{C}$.
($\mathcal{C}$3) $\mathcal{C}$ is closed under forming finite direct products, that is, if $G_i \in \mathcal{C}$ ($i = 1, \dots, n$), then

$$\prod_{i=1}^{n} G_i \in \mathcal{C}.$$

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4_2,

($\mathcal{C}4$) If G is a finite group with normal subgroups N_1 and N_2 such that $G/N_1, G/N_2 \in \mathcal{C}$, then $G/N_1 \cap N_2 \in \mathcal{C}$. Equivalently, $\mathcal{C}$ is closed under taking finite subdirect products, that is, if $G_i \in \mathcal{C}$, $(i = 1, \dots, n)$ and G is a subdirect product of $G_1, \dots, G_n$, then $G \in \mathcal{C}$.

($\mathcal{C}5$) $\mathcal{C}$ is *closed under extensions*, that is, if

$$1 \longrightarrow K \stackrel{\varphi}{\longrightarrow} G \stackrel{\psi}{\longrightarrow} H \longrightarrow 1$$

is a *short exact sequence* of groups (that is, φ is a monomorphism, ψ is an epimorphism and $\mathrm{Im}\,(\varphi) = \mathrm{Ker}(\psi)$) and $K, H \in \mathcal{C}$, then $G \in \mathcal{C}$.

Note that ($\mathcal{C}1$) plus ($\mathcal{C}3$) imply ($\mathcal{C}4$); ($\mathcal{C}4$) implies ($\mathcal{C}3$); and ($\mathcal{C}5$) implies ($\mathcal{C}3$).

For example, $\mathcal{C}$ could be the class of all

(a) finite groups; then $\mathcal{C}$ satisfies conditions ($\mathcal{C}1$)–($\mathcal{C}5$). In this case we call a pro-$\mathcal{C}$ group *profinite*. Observe that every pro-$\mathcal{C}$ group is also profinite.
(b) finite cyclic groups; then $\mathcal{C}$ satisfies conditions ($\mathcal{C}1$) and ($\mathcal{C}2$), but not ($\mathcal{C}3$), ($\mathcal{C}4$), ($\mathcal{C}5$). In this case we call a pro-$\mathcal{C}$ group *procyclic*.
(c) finite solvable groups; then $\mathcal{C}$ satisfies conditions ($\mathcal{C}1$)–($\mathcal{C}5$). In this case we call a pro-$\mathcal{C}$ group *prosolvable*.
(d) finite abelian groups; then $\mathcal{C}$ satisfies conditions ($\mathcal{C}1$)–($\mathcal{C}4$), but not ($\mathcal{C}5$). In this case we call a pro-$\mathcal{C}$ group *proabelian*.
(e) finite nilpotent groups; then $\mathcal{C}$ satisfies conditions ($\mathcal{C}1$)–($\mathcal{C}4$), but not ($\mathcal{C}5$). In this case we call a pro-$\mathcal{C}$ group *pronilpotent*.
(f) finite p-groups, for fixed prime number p; then $\mathcal{C}$ satisfies conditions ($\mathcal{C}1$)–($\mathcal{C}5$). In this case we call a pro-$\mathcal{C}$ group *pro-p*.

To avoid repetitions we shall give special names to classes $\mathcal{C}$ of finite groups satisfying some of the above conditions that are frequently used in this book.

- A *formation* of finite groups is a nonempty class of finite groups $\mathcal{C}$ that satisfies ($\mathcal{C}2$) and ($\mathcal{C}4$).
- A *variety* of finite groups is a nonempty class of finite groups $\mathcal{C}$ that satisfies conditions ($\mathcal{C}1$)–($\mathcal{C}3$).
- An NE-*formation* is a formation which is closed under taking normal subgroups and extensions.
- An *extension closed variety* is a variety which is closed under taking extensions.

Remark that a variety is automatically a formation, and that a subgroup closed formation is a variety.

Let Δ be a nonempty set of finite simple groups. A *Δ-group* D is a finite group whose composition factors are in Δ, that is, D is a finite group that has a composition series

$$D = D_0 \geq D_1 \geq \cdots \geq D_r = 1$$

such that $D_i/D_{i+1} \in \Delta$. If Δ consists only of one group S, we sometimes refer to Δ-groups as S-*groups*. Define $\mathcal{C} = \mathcal{C}(\Delta)$ to be the class of all Δ-groups; we sometimes refer to $\mathcal{C}(\Delta)$ as a Δ-*class*. Note that $\mathcal{C}(\Delta)$ is a formation closed under taking normal subgroups and extensions, that is, $\mathcal{C}(\Delta)$ is an NE-formation which is not necessarily subgroup closed. Conversely, if $\mathcal{C}$ is an NE-formation, then $\mathcal{C} = \mathcal{C}(\Delta)$, where Δ is the set of all simple groups in $\mathcal{C}$.

There are varieties of finite groups that are not of the form $\mathcal{C}(\Delta)$ (e.g., the variety of all finite nilpotent groups). And not every class of the form $\mathcal{C}(\Delta)$ is a variety (e.g., if Δ consists of a single finite simple nonabelian group S). Some important classes of extension closed varieties of finite groups are: the class of all finite groups, the class of all finite solvable groups and the class of all finite p-groups (for a fixed prime p).

Furthermore, if Δ is a set of nonabelian finite simple groups, then the class $\mathcal{S}$ of all finite groups which are direct products of groups in Δ is a formation which is not a variety nor a class of the form $\mathcal{C}(\Delta)$.

Lemma 2.1.1 *Let*

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

where $\{G_i, \varphi_{ij}, I\}$ *is an inverse system of finite groups* G_i, *and let*

$$\varphi_i : G \longrightarrow G_i \quad (i \in I)$$

be the projection homomorphisms. Then

$$\{S_i \mid S_i = \mathrm{Ker}(\varphi_i)\}$$

is a fundamental system of open neighborhoods of the identity element 1 *in* G.

Proof. Consider the family of neighborhoods of 1 in $\prod_{i \in I} G_i$ of the form

$$\left(\prod_{i \neq i_1, \ldots, i_t} G_i\right) \times \{1\}_{i_1} \times \cdots \times \{1\}_{i_t},$$

for any finite collection of indexes $i_1, \ldots, i_t \in I$, where $\{1\}_i$ denotes the subset of G_i consisting of the identity element. Since each G_i is discrete, this family is a fundamental system of neighborhoods of the identity element of $\prod_{i \in I} G_i$. Let $i_0 \in I$ be such that $i_0 \succeq i_1, \ldots, i_t$. Then

$$G \cap \left[\left(\prod_{i \neq i_0} G_i\right) \times \{1\}_{i_0}\right] = G \cap \left[\left(\prod_{i \neq i_1, \ldots, i_t} G_i\right) \times \{1\}_{i_1} \times \cdots \times \{1\}_{i_t}\right].$$

Therefore the family of neighborhoods of 1 in G, of the form

$$G \cap \left[\left(\prod_{i \neq i_0} G_i\right) \times \{1\}_{i_0}\right]$$

is a fundamental system of open neighborhoods of 1. Finally, observe that

$$G \cap \left[\left(\prod_{i \neq i_0} G_i \right) \times \{1\}_{i_0} \right] = \mathrm{Ker}(\varphi_{i_0}) = S_{i_0}.$$

□

We state next an easy consequence of compactness that will be used often without an explicit reference.

Lemma 2.1.2 *In a compact topological group G, a subgroup U is open if and only if U is closed of finite index.*

Let H be a subgroup of a group G. We define the *core* H_G of H in G to be the largest normal subgroup of G contained in H. Equivalently,

$$H_G = \bigcap_{g \in G} H^g,$$

where $H^g = g^{-1}Hg$. Observe that $H_G = \bigcap H^g$, where g ranges through a right transversal of H in G, that is, a set of representatives of the right cosets of H in G. Therefore, if H has finite index in G, then its core H_G has finite index in G. In particular, if H is an open subgroup of a profinite group G, then H_G is an open normal subgroup of G contained in H.

The following analog of Theorem 1.1.12 provides useful characterizations of pro-$\mathcal{C}$ groups.

Theorem 2.1.3 *Let $\mathcal{C}$ be a formation of finite groups. Then the following conditions on a topological group G are equivalent.*

(a) *G is a pro-$\mathcal{C}$ group;*
(b) *G is compact Hausdorff totally disconnected, and for each open normal subgroup U of G, $G/U \in \mathcal{C}$;*
(c) *G is compact and the identity element 1 of G admits a fundamental system $\mathcal{U}$ of open neighborhoods U such that $\bigcap_{U \in \mathcal{U}} U = 1$ and each U is an open normal subgroup of G with $G/U \in \mathcal{C}$;*
(d) *The identity element 1 of G admits a fundamental system $\mathcal{U}$ of open neighborhoods U such that each U is a normal subgroup of G with $G/U \in \mathcal{C}$, and*

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

Proof. (a) ⇒ (b): Say

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

where $\{G_i, \varphi_{ij}, I\}$ is a surjective inverse system of groups in $\mathcal{C}$. Denote by $\varphi_i : G \longrightarrow G_i$ $(i \in I)$ the projection homomorphisms. According to Theorem 1.1.12, G is compact Hausdorff and totally disconnected. Let U be an open normal subgroup G. By Lemma 2.1.1, there is some $S_i = \mathrm{Ker}(\varphi_i)$ with

$S_i \leq U$. Hence G/U is a quotient group of G/S_i. Since $G/S_i \in \mathcal{C}$ and $\mathcal{C}$ is closed under taking quotients, we have that $G/U \in \mathcal{C}$.

(b) ⇒ (c): By Theorem 1.1.12, the set $\mathcal{V}$ of clopen neighborhoods of 1 in G is a fundamental system of open neighborhoods of 1 and

$$\bigcap_{V \in \mathcal{V}} V = 1.$$

Therefore, it suffices to show that if V is a clopen neighborhood of 1, then it contains an open normal subgroup of G.

If X is a subset of G and n a natural number, for the purpose of this proof only, we denote by X^n the set of all products $x_1 \cdots x_n$, where $x_1, \ldots, x_n \in X$; further, denote by X^{-1} the set of all elements x^{-1}, where $x \in X$.

Set $F = (G - V) \cap V^2$. Since V is compact, so is V^2; hence, F is closed and therefore compact. Let $x \in V$; then $x \in G - F$. By the continuity of multiplication, there exists open neighborhoods V_x and S_x of x and 1 respectively such that $V_x, S_x \subseteq V$ and $V_x S_x \subseteq G - F$. By the compactness of V, there exist finitely many $x_1, \ldots, x_n$ such that $V_{x_1}, \ldots, V_{x_n}$ cover V. Put $S = \bigcap_{i=1}^n S_{x_i}$, and let $W = S \cap S^{-1}$. Then W is a symmetric neighborhood of 1 (that is, $w \in W$ if and only if $w^{-1} \in W$), $W \subseteq V$, and $VW \subseteq G - F$. Therefore $VW \cap F = \emptyset$. Since one also has that $VW \subseteq V^2$, we infer that $VW \cap (G - V) = \emptyset$; so $VW \subseteq V$. Consequently,

$$VW^n \subseteq V,$$

for each $n \in \mathbf{N}$. Since W is symmetric, it follows that

$$R = \bigcup_{n \in \mathbf{N}} W^n$$

is an open subgroup of G contained in V. Thus the core of R

$$R_G = \bigcap_{x \in G} (x^{-1} R x)$$

is an open normal subgroup of G. Finally, observe that $R_G \subseteq V$ because

$$R_G \leq R \subseteq VR \subseteq \bigcup_{n \in \mathbf{N}} VW^n \subseteq V.$$

Thus R_G is the desired open normal subgroup contained in V.

(c) ⇒ (d): Let $\mathcal{U}$ be as in (c). Make $\mathcal{U}$ into a directed poset by defining $U \succeq V$ if $U \leq V$, for $U, V \in \mathcal{U}$. Consider the inverse system $\{G/U, \varphi_{UV}\}$, of all groups G/U ($U \in \mathcal{U}$) where $\varphi_{UV} : G/U \longrightarrow G/V$ is the natural epimorphism for $U \succeq V$. Since the canonical epimorphisms

$$\psi_U : G \longrightarrow G/U$$

are compatible, they induce a continuous homomorphism

$$\psi : G \longrightarrow \varprojlim_{U \in \mathcal{U}} G/U.$$

We shall show that ψ is an isomorphism of topological groups. According to Corollary 1.1.6, ψ is an epimorphism. To see that ψ is a homeomorphism, it suffices to prove that ψ is a monomorphism since G is compact. Now, if $x \in G$ and $\psi(x) = 1$, then $x \in U$ for each $U \in \mathcal{U}$. Since

$$\bigcap_{U \in \mathcal{U}} U = 1,$$

it follows that $x = 1$, as needed.

The implication (d) $\Rightarrow$ (a) is clear. □

We say that a collection $\mathcal{S}$ of subsets of a group G is *filtered from below* if for every pair of subsets $S_1, S_2 \in \mathcal{S}$, there exists some $S_3 \in \mathcal{S}$ with $S_3 \leq S_1 \cap S_2$.

Proposition 2.1.4 *Let H be a closed subgroup of a profinite group G.*

(a) *If $\{U_i \mid i \in I\}$ is a family of closed subsets of G filtered from below, then*

$$\bigcap_{i \in I} HU_i = H\Big(\bigcap_{i \in I} U_i\Big).$$

(b) *Let $\varphi : G \longrightarrow R$ be a continuous epimorphism of profinite groups. Assume that $\{U_i \mid i \in I\}$ is a family of closed subsets of G filtered from below. Then*

$$\varphi\Big(\bigcap_{i \in I} U_i\Big) = \bigcap_{i \in I} \varphi(U_i).$$

(c) *Every open subgroup of G that contains H, contains an open subgroup of the form HU for some open normal subgroup U of G.*

(d) *H is the intersection of all open subgroups of G containing H. If H is normal in G, then H is the intersection of all open normal subgroups of G containing H.*

Proof. (a) By the filtration assumption, the result is clearly true if the set I is finite. For the general case, it is plain that $\bigcap_{i \in I} HU_i \geq H(\bigcap_{i \in I} U_i)$. Let $x \in \bigcap_{i \in I} HU_i$ and let $\{J_t \mid t \in T\}$ be the collection of all finite subsets J_t of I such that $\{U_j \mid j \in J_t\}$ is filtered from below. Then, for each $t \in T$, $x \in \bigcap_{i \in J_t} HU_j = H(\bigcap_{j \in J_t} U_j)$ and so, $Hx \cap (\bigcap_{j \in J_t} U_j) \neq \emptyset$. Therefore, by the finite intersection property of the compact space G, we have

$$Hx \cap \Big(\bigcap_{i \in I} U_i\Big) = \bigcap_{t \in T} \Big(Hx \cap \Big(\bigcap_{j \in J_t} U_j\Big)\Big) \neq \emptyset.$$

Thus $x \in H(\bigcap_{i\in I} U_i)$, as needed.

(b) Let $H = \mathrm{Ker}(\varphi)$ and identify R with G/H. Then, using part (a),

$$\bigcap_{i\in I} \varphi(U_i) = \bigcap_{i\in I}(U_iH/H) = \Big(\bigcap_{i\in I} U_iH\Big)/H = \Big(\bigcap_{i\in I} U_i\Big)H/H = \varphi\Big(\bigcap_{i\in I} U_i\Big).$$

(c) Let V be an open subgroup of G containing H. Then its core

$$V_G = \bigcap_{g\in G} V^g$$

is open and normal; moreover $HV_G \le V$.

(d) This follows from parts (a) and (c) by taking $\{U_i \mid i \in I\}$ in (a) to be the collection of all open normal subgroups of G. □

From now on we shall use the following convenient notations. Let G be a topological group and H a subgroup of G. Then

$$H \le_o G, \qquad H \le_c G, \qquad H \triangleleft_o G, \qquad H \triangleleft_c G, \qquad H \le_f G, \qquad H \triangleleft_f G,$$

will indicate respectively: H is an open subgroup, H is a closed subgroup, H is an open normal subgroup, H is a closed normal subgroup of G, H is a subgroup of finite index, H is a normal subgroup of finite index.

Proposition 2.1.5

(a) *Let $\{H_i \mid i \in I\}$ be a collection of closed subgroups of a profinite group G and let $\bigcap_{i\in I} H_i \le U \le_o G$. Then there is some finite subset J of I such that $\bigcap_{j\in J} H_j \le U$.*

(b) *Let $\{U_i \mid i \in I\}$ be a collection of open subgroups of a profinite group G such that $\bigcap_{i\in I} U_i = 1$. Let*

$$\mathcal{V} = \Big\{\bigcap_{j\in J} U_j \mid J \text{ a finite subset of } I\Big\}.$$

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

Proof. Part (b) follows immediately from (a). To prove (a), consider the open covering $\{G-H_i \mid i \in I\}$ of the compact space $G-U$. Choose a finite subcover, say $\{G - H_j \mid i \in J\}$. Then $G - U \subseteq \bigcup_{j\in J}(G - H_j)$. Thus $\bigcap_{j\in J} H_j \subseteq U$. □

Example 2.1.6 (Completions)

(1) Let $\mathcal{C}$ be a fixed formation of finite groups, and let G be a group. Consider the collection

$$\mathcal{N} = \{N \triangleleft_f G \mid G/N \in \mathcal{C}\}.$$

Note that $\mathcal{N}$ is nonempty since $G \in \mathcal{N}$. Make $\mathcal{N}$ into a directed poset by defining $M \preceq N$ if $M \ge N$ $(M, N \in \mathcal{N})$. If $M, N \in \mathcal{N}$ and $N \succeq M$, let

$\varphi_{NM} : G/N \longrightarrow G/M$ be the natural epimorphism. Then

$$\{G/N, \varphi_{NM}\}$$

is an inverse system of groups in $\mathcal{C}$, and we say that the pro-$\mathcal{C}$ group

$$G_{\hat{\mathcal{C}}} = \varprojlim_{N \in \mathcal{N}} G/N$$

is the *pro-$\mathcal{C}$ completion* of G (we shall give a description of completion in Section 3.2 in a more general setting; there we introduce also the notation $\mathcal{K}_{\mathcal{C}}(G)$ for $G_{\hat{\mathcal{C}}}$). In particular we use the terms *profinite completion*, the *pro-p completion*, the *pronilpotent completion*, etc., in the cases where $\mathcal{C}$ consists of all finite groups, all finite p-groups, all finite nilpotent groups, etc., respectively. The profinite and pro-p completions of a group of G appear quite frequently, and they will be usually denoted instead by $\widehat{G}$, and $G_{\hat{p}}$, respectively.

(2) As a special case of (1), consider the group of integers $\mathbf{Z}$. Its profinite completion is

$$\widehat{\mathbf{Z}} = \varprojlim_{n \in \mathbf{N}} \mathbf{Z}/n\mathbf{Z}.$$

Following a long tradition in Number Theory, we shall denote the pro-p completion of $\mathbf{Z}$ by $\mathbf{Z}_p$ rather than $\mathbf{Z}_{\hat{p}}$. So,

$$\mathbf{Z}_p = \varprojlim_{n \in \mathbf{N}} \mathbf{Z}/p^n\mathbf{Z}.$$

Observe that both $\widehat{\mathbf{Z}}$ and $\mathbf{Z}_p$ are not only abelian groups, but also they inherit from the finite rings $\mathbf{Z}/n\mathbf{Z}$ and $\mathbf{Z}/p^n\mathbf{Z}$ respectively, natural structures of rings. The group (ring) $\mathbf{Z}_p$ is called the group (ring) of *p-adic integers*.

(3) Let R be a profinite ring with 1, that is, R is a compact Hausdorff totally disconnected topological ring with 1. Assume in addition that R is commutative (e.g., R could be $\widehat{\mathbf{Z}}$ or $\mathbf{Z}_p$). Then one easily checks that the following groups (with topologies naturally induced from R) are profinite groups:

- $R^\times$, the group of units of R [one can verify the compactness of $R^\times$ as follows: consider the multiplication mapping $\mu : R \times R \longrightarrow R$; then $\mu^{-1}\{1\}$ is compact; on the other hand, $R^\times$ is the image of $\mu^{-1}\{1\}$ under one of the projections $R \times R \longrightarrow R$].
- $\mathrm{GL}_n(R)$ (the group of invertible $n \times n$ matrices with entries from R, i.e., the group of units of the ring $M_n(R)$ of all $n \times n$ matrices over R). [One can verify this as in the previous case, eventhough $M_n(R)$ is not commutative: just observe that, for matrices over R, having a left inverse is equivalent to being invertible].
- $\mathrm{SL}_n(R)$ (the subgroup of $\mathrm{GL}_n(R)$ of those matrices of determinant 1).

(4) The upper unitriangular group over $\mathbf{Z}_p$ of degree n

$$\mathrm{UT}_n(\mathbf{Z}_p) = \left\{ \begin{pmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ 0 & 0 & 1 & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \middle| \, a_{ij} \in \mathbf{Z}_p \right\}$$

is a pro-p group.

Exercise 2.1.7 A proabelian group is necessarily abelian. But a pronilpotent (respectively, prosolvable) group need not be nilpotent (respectively, solvable).

Exercise 2.1.8

(1) The set of elements of $\widehat{\mathbf{Z}}$ can be identified with the set of all (equivalence classes of) sequences $(a_n) = (a_1, a_2, a_3, \dots)$ of natural numbers such that

$$a_n \equiv a_m \pmod{m}$$

whenever $m \mid n$. Explain this identification and what is the addition and multiplication of these sequences under the identification. Show that every element t of $\mathbf{Z}$ can be identified with a constant sequence (a_n), $a_n = t$ for all $n = 1, 2, \dots$.

(2) Similarly, the set of elements of $\mathbf{Z}_p$ can be identified with the set group of all (equivalence classes of) sequences $(a_n) = (a_1, a_2, a_3, \dots)$ of natural numbers such that

$$a_n \equiv a_m \pmod{p^m}$$

whenever $m \leq n$. Explain this identification and what is the addition and multiplication of these sequences under the identification.

(3) Show that $\mathbf{Z}_p$ can also be identified with the set of power series

$$\mathbf{Z}_p = \left\{ b = \sum_{n=0}^{\infty} b_n p^n \mid b_n \in \mathbf{N}, \ 0 \leq b_n < p \right\}.$$

Explain how the addition and multiplication of series is carried out under this identification. How is $\mathbf{Z}$ embedded in $\mathbf{Z}_p$ under this identification?

(4) Show that an element $b \in \mathbf{Z}_p$ is a unit in the ring $\mathbf{Z}_p$ if and only if in its series representation $b = \sum_{n=0}^{\infty} b_n p^n$ in (3) one has $b_0 \neq 0$.

Exercise 2.1.9

(1) Prove that for each natural number i, there is a short exact sequence of profinite groups

$$I \longrightarrow K_i \longrightarrow \mathrm{GL}_n(\mathbf{Z}_p) \xrightarrow{\varphi_i} \mathrm{GL}_n(\mathbf{Z}/p^i\mathbf{Z}) \longrightarrow I$$

where φ_i is induced by the canonical epimorphism $\mathbf{Z}_p \longrightarrow \mathbf{Z}/p^i\mathbf{Z}$, and $K_i = I + M_n(p^i\mathbf{Z})$ (I denotes here the $n \times n$ identity matrix over $\mathbf{Z}_p$, and $M_n(p^i\mathbf{Z})$ all the $n \times n$ matrices with entries in $p^i\mathbf{Z}$). [Hint: observe that $b \in \mathbf{Z}_p$ is unit if and only if its image in $\mathbf{Z}/p^i\mathbf{Z}$ is a unit.]

(2) Show that $\bigcap K_i = \{I\}$, and deduce that

$$\mathrm{GL}_n(\mathbf{Z}_p) = \varprojlim_i \mathrm{GL}_n(\mathbf{Z}/p^i\mathbf{Z}).$$

2.2 Basic Properties of Pro-$\mathcal{C}$ Groups

We begin with some elementary properties of pro-$\mathcal{C}$ groups inherited from corresponding properties of $\mathcal{C}$.

Proposition 2.2.1 *Let $\mathcal{C}$ be a formation of finite groups. Then*

(a) *Every quotient group G/K of a pro-$\mathcal{C}$ group G, where $K \triangleleft_c G$, is a pro-$\mathcal{C}$ group. If, in addition, $\mathcal{C}$ is closed under taking subgroups (respectively, under taking normal subgroups), then every closed subgroup (respectively, every closed normal subgroup) of G is a pro-$\mathcal{C}$ group.*

(b) *The direct product $\prod_{i\in I} G_i$ of any collection $\{G_j \mid i \in J\}$ of pro-$\mathcal{C}$ groups with the product topology is a pro-$\mathcal{C}$ group.*

(c) *If a profinite group is a subdirect product of pro-$\mathcal{C}$ groups, then it is pro-$\mathcal{C}$.*

(d) *The inverse limit*

$$\varprojlim_{i\in I} G_i,$$

of a surjective inverse system $\{G_i, \varphi_{ij}, I\}$ of pro-$\mathcal{C}$ groups, is a pro-$\mathcal{C}$ group.

(e) *Let $\mathcal{C}$ be an extension closed variety of finite groups. Then the class of pro-$\mathcal{C}$ groups is closed under extensions.*

Proof. (a) This is an easy application of Corollary 1.1.8 and Theorem 2.1.3.

(b) Let $G = \prod_{i\in I} G_i$, where each G_i is a pro-$\mathcal{C}$ group. Then G is a compact, Hausdorff and totally disconnected group (the compactness is a consequence of Tychonoff's Theorem: see for example Bourbaki [1989], Ch. 1, Theorem 3). Hence G is a profinite group. Let $U \triangleleft_o G$. To verify that G is pro-$\mathcal{C}$ we must show that $G/U \in \mathcal{C}$, according to Theorem 2.1.3. By definition of the product topology, there exist a finite subset J of I and open normal subgroups U_j of G_j ($j \in J$) such that $U \geq \prod_{i\in I} X_i$, where $X_i = U_i$ for $i \in J$ and $X_i = G_i$ for $i \in I - J$. So G/U is a homomorphic image of the group

$$G/\prod_{i\in I} X_i \cong \prod_{j\in J} G_j/U_j.$$

Since $\mathcal{C}$ is a formation and $G_j/U_j \in \mathcal{C}$ ($j \in J$), one has that $G/U \in \mathcal{C}$.

(c) Let G be a profinite group and let $\{N_i \mid i \in I\}$ be a collection of closed normal subgroups of G such that G/N_i is pro-$\mathcal{C}$ for each $i \in I$, and $\bigcap_{i\in I} N_i = 1$. We must show that G is a pro-$\mathcal{C}$ group. In order to do this, it suffices to show that $G/U \in \mathcal{C}$ whenever $U \triangleleft_o G$. Let $J \subseteq_f I$ indicate that J is a finite subset of I. For $J \subseteq_f I$, define $N_J = \bigcap_{j\in J} N_j$. Since $N_J \triangleleft_c G$, the group G/N_J is pro-$\mathcal{C}$. Note that the collection $\{N_J \mid J \subseteq_f I\}$ of closed normal subgroups of G is filtered from below. Hence, $\bigcap_{J\subseteq_f I}(N_J U/U) = 1$ in G/U (see Proposition 2.1.4). Therefore, G/U is a subdirect product of the (finite) set of groups $\{(G/U)/(N_J U/U) \cong G/N_J U \mid J \subseteq_f I\}$. Since $G/N_J U$ is a quotient of G/N_J, we deduce that $G/N_J U \in \mathcal{C}$. Thus, using the fact that $\mathcal{C}$ is a formation of finite groups, we get $G/U \in \mathcal{C}$, as needed.

(d) follows from (b) and (a)

(e) Let

$$1 \longrightarrow K \longrightarrow E \xrightarrow{\varphi} G \longrightarrow 1$$

be an exact sequence of profinite groups and assume that K and G are pro-$\mathcal{C}$. Let $U \triangleleft_o E$. Then the induced sequence of finite groups

$$1 \longrightarrow KU/U \longrightarrow E/U \xrightarrow{\bar{\varphi}} G/\varphi(U) \longrightarrow 1$$

is exact. Since $KU/U \cong K/K \cap U$ and $G/\varphi(U)$ are in $\mathcal{C}$, it follows that $E/U \in \mathcal{C}$. Hence E is a pro-$\mathcal{C}$ group (see Theorem 2.1.3). $\square$

Existence of Sections

Let $\varphi : X \longrightarrow Y$ be an epimorphism of sets. We say that a map $\sigma : Y \longrightarrow X$ is a *section* of φ if $\varphi\sigma = \mathrm{id}_Y$. Plainly every epimorphism φ of sets admits a section. However, if X and Y are topological spaces and φ is continuous, it is not necessarily true that φ admits a continuous section. For example, the natural epimorphism $\mathbf{R} \longrightarrow \mathbf{R}/\mathbf{Z}$ from the group of real numbers to the circle group does not admit a continuous section. Nevertheless, every epimorphism of profinite groups admits a continuous section, as the following proposition shows.

Proposition 2.2.2 *Let H be a closed normal subgroup of a profinite group G, and let*

$$\pi : G \longrightarrow G/H$$

be the canonical projection. Then π admits a continuous section

$$\sigma : G/H \longrightarrow G$$

with the property that $\sigma(1H) = 1$.

Proof. We divide the proof into two parts. Assume first that H is a finite group. Then there exists an open normal subgroup U of G such that $U \cap H = 1$. Therefore the restriction $\pi|_U$ is injective. Since U is compact, the restriction $\pi|_U : U \longrightarrow \pi(U)$ is an isomorphism of topological groups. Hence, there is a continuous inverse isomorphism $\sigma : \pi(U) \longrightarrow U$ of $\pi|_U$. Since $\pi(U)$ is an open (normal) subgroup of G/H, one can express G/H as a finite disjoint union of the left cosets of $\pi(U)$. Consequently, σ admits a continuous extension, by translation, to the whole of G/H. This extension is a section of π, which we denote still by σ. Clearly, $\sigma(1H) = 1$.

Consider now the general case, that is, H is any closed normal subgroup of G. Let $\mathcal{P}$ be the set of all pairs (L, η), where L is a closed normal subgroup of G with $L \le H$, and where $\eta : G/H \longrightarrow G/L$ is a continuous section of the natural projection $G/L \longrightarrow G/H$ such that $\eta(1H) = 1L$. Clearly $\mathcal{P}$ is nonempty, since $(H, \mathrm{id}_{G/H}) \in \mathcal{P}$. Define a partial ordering on $\mathcal{P}$ as follows:

$$(K_1, \eta_1) \succeq (K_2, \eta_2) \quad \text{if } K_1 \le K_2,$$

and the diagram

$$\begin{array}{ccc} G/K_1 & \longrightarrow & G/K_2 \\ {\scriptstyle \eta_1}\nwarrow & & \nearrow{\scriptstyle \eta_2} \\ & G/H & \end{array}$$

commutes, where the horizontal map is the natural epimorphism. In order to apply Zorn's lemma, we show next that $\mathcal{P}$ is an inductive poset. If

$$\{(K_i, \eta_i) \mid i \in I\}$$

is a linearly ordered subset of $\mathcal{P}$, set $K = \bigcap_{i \in I} K_i$; then one easily checks that

$$G/K = \varprojlim_{I} G/K_i.$$

Since the mappings $\{\eta_i \mid i \in I\}$ are compatible, they induce a continuous mapping

$$\eta : G/H \longrightarrow G/K.$$

Then $(K, \eta) \in \mathcal{P}$ and $(K, \eta) \succeq (K_i, \eta_i)$, for every $i \in I$. So $\{(K_i, \eta_i) \mid i \in I\}$ has an upper bound in $\mathcal{P}$, and thus $\mathcal{P}$ is inductive. Therefore, by Zorn's lemma, there is a maximal element (T, σ) of $\mathcal{P}$. To see that σ is the desired section, it will suffice to show that $T = 1$. If this were not the case, there would exist an open normal subgroup U of G with $U \cap T < T$. We prove that this leads to a contradiction by exhibiting a continuous section

$$\zeta : G/H \longrightarrow G/(U \cap T)$$

of $G/(U \cap T) \longrightarrow G/H$ such that $(U \cap T, \zeta) \succ (T, \sigma)$. To show the existence of ζ, it suffices to find a continuous section

$$\xi : G/T \longrightarrow G/(U \cap T)$$

to the projection

$$G/(U \cap T) \longrightarrow G/T.$$

But $G/T = (G/(U \cap T))/(T/(U \cap T))$, and $T/(U \cap T)$ is a finite group. Thus the existence of ξ follows from the first part of the proof. $\square$

Exercise 2.2.3 Let $K \leq H$ be closed (not necessarily normal) subgroups of a profinite group G. Consider the natural continuous epimorphism of topological spaces

$$\pi : G/K \longrightarrow G/H.$$

Prove that π admits a continuous section $\sigma : G/H \longrightarrow G/K$ such that $\sigma(1H) = 1K$.

Exactness of Inverse Limits of Profinite Groups

Let

$$1 \longrightarrow \{G_i, \varphi_{ij}, I\} \stackrel{\Theta}{\longrightarrow} \{G_i', \varphi_{ij}', I\} \stackrel{\Psi}{\longrightarrow} \{G_i'', \varphi_{ij}'', I\} \longrightarrow 1 \qquad (1)$$

be a sequence of inverse systems of profinite groups over the same directed poset I and maps of inverse systems. Say $\Theta = \{\theta_i\}$ and $\Psi = \{\psi_i\}$, and assume that for each $i \in I$ the corresponding short sequence of profinite groups

$$1 \longrightarrow G_i \stackrel{\theta_i}{\longrightarrow} G_i' \stackrel{\psi_i}{\longrightarrow} G_i'' \longrightarrow 1$$

is exact, that is, θ_i is a monomorphism, ψ_i is an epimorphism, and $\mathrm{Im}(\theta_i) = \mathrm{Ker}(\psi_i)$. In this situation we say that the sequence (1) is a *short exact sequence* of inverse systems of profinite groups. If we apply the functor $\varprojlim$ to this sequence, we get a sequence of groups and continuous homomorphisms

$$1 \longrightarrow \varprojlim_{i \in I} G_i \stackrel{\theta}{\longrightarrow} \varprojlim_{i \in I} G_i' \stackrel{\psi}{\longrightarrow} \varprojlim_{i \in I} G_i'' \longrightarrow 1, \qquad (2)$$

where $\theta = \varprojlim \theta_i$ and $\psi = \varprojlim \psi_i$. We claim that (2) is a short exact sequence of profinite groups. Indeed, θ is obviously a monomorphism and, by Lemma 1.1.5, ψ is onto. Furthermore, $\mathrm{Im}(\theta) = \mathrm{Ker}(\psi)$, for clearly $\psi\theta(x_i) = 1$ for all $(x_i) \in \varprojlim G_i$; hence $\mathrm{Im}(\theta) \leq \mathrm{Ker}(\psi)$. Conversely, assume that $(x_i') \in \mathrm{Ker}(\psi)$; then for each $i \in I$, there exists $x_i \in G_i$ with $\theta(x_i) = x_i'$. Since the θ_i are monomorphisms commuting with the maps φ_{ij} and φ_{ij}', we deduce that $(x_i) \in \varprojlim G_i$; so $\theta(x_i) = (x_i')$. Therefore, $\mathrm{Im}(\theta) \supseteq \mathrm{Ker}(\psi)$. This proves the claim.

A functor that preserves exactness in this way, is called an *exact functor*. Hence we have proved the following result.

Proposition 2.2.4 *Consider the functor $\varprojlim$ from the category of inverse systems of profinite groups over the same directed poset I to the category of profinite groups. Then $\varprojlim$ is exact.*

2.3 The Order of a Profinite Group and Sylow Subgroups

We begin this section by showing that an infinite profinite group cannot be countable. This is a general fact for locally compact topological groups, but here we present a proof for profinite groups only. The first part of the following proposition is a special case of the classical Baire category theorem, valid for locally compact spaces.

Proposition 2.3.1 *Let G be a profinite group.*

(a) *Let $C_1, C_2, \ldots$ be a countably infinite set of nonempty closed subsets of G having empty interior. Then*

$$G \neq \bigcup_{n=1}^{\infty} C_i.$$

(b) *The cardinality $|G|$ of G is either finite or uncountable.*

Proof. Part (b) follows immediately from (a). To prove (a), assume that $G = \bigcup_{i=1}^{\infty} C_i$, where each C_i is a nonempty closed subset of G with empty interior. Then $D_i = G - C_i$ is a dense open subset of G, for each $i = 1, 2, \ldots$.

Next consider a nonempty open subset U_0 of G; then $U_0 \cap D_1$ is open and nonempty since D_1 is open and dense in G. By Theorem 1.1.12(c), there is a nonempty clopen subset U_1 of $U_0 \cap D_1$. Similarly, $U_1 \cap D_2$ is open and nonempty; therefore there is a nonempty clopen subset U_2 of $U_1 \cap D_2$. Proceeding in this manner we obtain a nested sequence of clopen nonempty subsets

$$U_1 \supseteq U_2 \supseteq \cdots \supseteq U_i \supseteq \cdots$$

such that $U_i \subseteq D_i \cap U_{i-1}$ for each $i = 1, 2, \ldots$. Since G is compact and the closed sets U_i have the finite intersection property, we have that

$$\bigcap_{i=1}^{\infty} U_i \neq \emptyset.$$

On the other hand,

$$\bigcap_{i=1}^{\infty} U_i \subseteq \bigcap_{i=1}^{\infty} D_i = G - \left(\bigcup_{i=1}^{\infty} C_i \right) = \emptyset,$$

a contradiction. □

Consider a profinite group

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

where each G_i is a finite group. If G is infinite, then the knowledge of its cardinality carries with it little information. There is, nevertheless, a very useful notion of order of a profinite group G that reflects, in a global manner, the arithmetic properties of the finite groups G_i and it is independent of the presentation of G as an inverse limit of finite groups. In order to explain this concept we need first to introduce the notion of supernatural number.

A *supernatural number* is a formal product

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

where p runs through the set of all prime numbers, and where $n(p)$ is a non-negative integer or ∞. By convention, we say that $n < \infty$, $\infty + \infty = \infty + n = n + \infty = \infty$ for all $n \in \mathbf{N}$. If

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

is another supernatural number, and $m(p) \leq n(p)$ for each p, then we say that m *divides* n, and we write $m \mid n$. If

$$\left\{ n_i = \prod_p p^{n(p,i)} \mid i \in I \right\}$$

is a collection of supernatural numbers, then we define their product, greatest common divisor and least common multiple in the following natural way

- $\prod_I n_i = \prod_p p^{n(p)}$, where $n(p) = \sum_i n(p,i)$;
- $\gcd\{n_i\}_{i \in I} = \prod_p p^{n(p)}$, where $n(p) = \min_i\{n(p,i)\}$;
- $\operatorname{lcm}\{n_i\}_{i \in I} = \prod_p p^{n(p)}$, where $n(p) = \max_i\{n(p,i)\}$.

(Here $\sum_i n(p,i)$, $\min_i\{n(p,i)\}$ and $\max_i\{n(p,i)\}$ have an obvious meaning; note that the results of these operations can be either non-negative integers or ∞.)

Let G be a profinite group and H a closed subgroup of G. Let $\mathcal{U}$ denote the set of all open normal subgroups of G. We define the *index* $[G : H]$ of H in G, to be the supernatural number

$$[G : H] = \operatorname{lcm}\{[G/U : HU/U] \mid U \in \mathcal{U}\}.$$

The *order* $\#G$ of G is the supernatural number $\#G = [G : 1]$, namely,

$$\#G = \operatorname{lcm}\{|G/U| \mid U \in \mathcal{U}\}.$$

Proposition 2.3.2 *Let G be a profinite group.*

(a) *If $H \leq_c G$, then $[G : H]$ is a natural number if and only if H is an open subgroup of G;*

(b) *If* $H \leq_c G$, *then*

$$[G:H] = \mathrm{lcm}\{[G:U] \mid H \leq U \leq_o G\};$$

(c) *If* $H \leq_c G$ *and* $\mathcal{U}'$ *is a fundamental system of neighborhoods of* 1 *in* G *consisting of open normal subgroups, then*

$$[G:H] = \mathrm{lcm}\{[G/U : HU/U] \mid U \in \mathcal{U}'\};$$

(d) *Let* $K \leq_c H \leq_c G$. *Then*

$$[G:K] = [G:H][H:K];$$

(e) *Let* $\{H_i \mid i \in I\}$ *be a family of closed subgroups of* G *filtered from below. Assume that* $H = \bigcap_{i\in I} H_i$. *Then*

$$[G:H] = \mathrm{lcm}\{[G:H_i] \mid i \in I\};$$

(f) *Let* $\{G_i, \varphi_{ij}\}$ *be a surjective inverse system of profinite groups over a directed poset* I. *Let* $G = \varprojlim_{i\in I} G_i$. *Then*

$$\#G = \mathrm{lcm}\{\#G_i \mid i \in I\};$$

(g) *For any collection* $\{G_i \mid i \in I\}$ *of profinite groups,*

$$\#\left(\prod_{i\in I} G_i\right) = \prod_{i\in I} \#G_i.$$

Proof. We shall prove only part (d), leaving the rest as exercises. Let $\mathcal{U}$ denote the collection of all open normal subgroups of G. Then

$$\begin{aligned}[G:K] &= \mathrm{lcm}\{[G/U : KU/U] \mid U \in \mathcal{U}\}\\ &= \mathrm{lcm}\{[G/U : HU/U][HU/U : KU/U] \mid U \in \mathcal{U}\}.\end{aligned}$$

Now, $\{H \cap U \mid U \in \mathcal{U}\}$ is a fundamental system of neighborhoods of 1 in H. So, by (c),

$$\begin{aligned}[H:K] &= \mathrm{lcm}\{[H/H\cap U : K(H\cap U)/H\cap U] \mid U \in \mathcal{U}\}\\ &= \mathrm{lcm}\{[HU/U : KU/U] \mid U \in \mathcal{U}\}.\end{aligned}$$

Hence, it suffices to prove that

$$\begin{aligned}&\mathrm{lcm}\{[G/U : HU/U][HU/U : KU/U] \mid U \in \mathcal{U}\}\\ &\quad = \mathrm{lcm}\{[G/U : HU/U] \mid U \in \mathcal{U}\}\ \mathrm{lcm}\{[HU/U : KU/U] \mid U \in \mathcal{U}\}.\end{aligned}$$

Let p be a prime number, and let p^n, p^{n_1} and p^{n_2} be the largest powers of p such that

$$p^n \mid \operatorname{lcm}\{[G/U : HU/U][HU/U : KU/U] \mid U \in \mathcal{U}\},$$
$$p^{n_1} \mid \operatorname{lcm}\{[G/U : HU/U] \mid U \in \mathcal{U}\}$$

and

$$p^{n_2} \mid \operatorname{lcm}\{[HU/U : KU/U] \mid U \in \mathcal{U}\},$$

respectively ($n, n_1, n_2 \in \mathbf{N} \cup \{\infty\}$). Then, clearly $n \leq n_1 + n_2$, $n \geq n_1$, and $n \geq n_2$. So, if $n = \infty$, $n = n_1 + n_2$. If $n < \infty$, it follows that $n_1, n_2 < \infty$. Then there exist $U_1, U_2 \in \mathcal{U}$ such that

$$p^{n_1} \mid [G/U_1 : HU_1/U_1] \quad \text{and} \quad p^{n_2} \mid [HU_2/U_2 : KU_2/U_2].$$

Let $U = U_1 \cap U_2$. Then $U \in \mathcal{U}$ and

$$p^{n_1+n_2} \mid [G/U : HU/U][HU/U : KU/U].$$

Hence $n \geq n_1 + n_2$, and thus $n = n_1 + n_2$, as needed. □

Let π be a set of prime numbers and let π' denote the set of those primes not in π. We say that a supernatural number

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

is a π-*number* if whenever $n(p) \neq 0$ then $p \in \pi$. A profinite group G is called a *pro-π group* or *π-group* if its order $\#G$ is a π-number, that is, if G is the inverse limit of finite groups whose orders are divisible by primes in π only. If $\pi = \{p\}$ consists of just the prime p, then we usually write pro-p group rather than pro-$\{p\}$ group. A closed subgroup H of a profinite group G is a *π-Hall subgroup* if $\#H$ is a π-number and $[G : H]$ is a π'-number. When $\pi = \{p\}$, a π-Hall subgroup is called a *p-Sylow subgroup*.

Exercise 2.3.3 Let π be a set of prime numbers and $\varphi : G \longrightarrow K$ a continuous homomorphism of profinite groups. Let $H \leq_c G$. Then

(a) If H is a π-group, so is $\varphi(H)$;
(b) If H is a π-Hall subgroup of G, then $\varphi(H)$ is a π-Hall subgroup of $\varphi(G)$.

Lemma 2.3.4 *Let π be a set of prime numbers. Assume that G is a profinite group and let H be a closed subgroup of G.*

(a) *Suppose that*

$$G = \varprojlim_I G_i,$$

where $\{G_i, \varphi_{ij}, I\}$ is a surjective inverse system of finite groups. Then, H is a π-Hall subgroup of G if and only if each $\varphi_i(H)$ is a π-Hall subgroup of G_i.

(b) *H is a π-Hall subgroup of G if and only if HU/U is a π-Hall subgroup of G/U for each open normal subgroup U of G.*

Proof. Part (b) follows from part (a). By Corollary 1.1.8,

$$H = \varprojlim_{I} \varphi_i(H).$$

So, by part (f) of the proposition above and Exercise 2.3.3, H is a π-group if and only if each $\varphi_i(H)$ is a π-group. Let $S_i = \mathrm{Ker}(\varphi_i)$. By Lemma 2.1.1, the collection of open normal subgroups $\{S_i \mid i \in I\}$ is a fundamental system of neighborhoods of 1 in G; hence, by Proposition 2.3.2(c),

$$[G : H] = \mathrm{lcm}\{[G/S_i : HS_i/S_i] \mid i \in I\}.$$

Since each φ_i is an epimorphism (see Proposition 1.1.10), $[G/S_i : HS_i/S_i] = [G_i : \varphi_i(H)]$. Thus, $[G : H]$ is a π'-number if and only if each $[G_i : \varphi_i(H)]$ is a π'-number. □

Theorem 2.3.5 *Let π be a fixed set of prime numbers and let*

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

be a profinite group, where $\{G_i, \varphi_{ij}, I\}$ is a surjective inverse system of finite groups. Assume that every group G_i $(i \in I)$ satisfies the following properties:

(a) *G_i contains a π-Hall subgroup*;
(b) *Any π-subgroup of G_i is contained in a π-Hall subgroup*;
(c) *Any two π-Hall subgroups of G_i are conjugate.*

Then

(a′) *G contains a π-Hall subgroup*;
(b′) *Any closed π-subgroup of G is contained in a π-Hall subgroup*;
(c′) *Any two π-Hall subgroups of G are conjugate.*

Proof. (a′) Let $\mathcal{H}_i$ be the set of all π-Hall subgroups of G_i. By (a), $\mathcal{H}_i \neq \emptyset$. Since φ_{ij} is an epimorphism, $\varphi_{ij}(\mathcal{H}_i) \subset \mathcal{H}_j$, whenever $i \succeq j$. Therefore, $\{\mathcal{H}_i, \varphi_{ij}, I\}$ is an inverse system of nonempty finite sets. Consequently, according to Proposition 1.1.4,

$$\varprojlim_{i \in I} \mathcal{H} \neq \emptyset.$$

Let $(H_i) \in \varprojlim \mathcal{H}_i$. Then H_i is a π-Hall subgroup of G_i for each $i \in I$, and $\{H_i, \varphi_{ij}, I\}$ is an inverse system of finite groups. Hence, by Lemma 2.3.4, $H = \varprojlim H_i$ is a π-Hall subgroup of G, as desired.

(b′) Let H be a π-subgroup of G. Then, $\varphi_i(H)$ is a π-subgroup of G_i $(i \in I)$. By assumption (b), there is some π-Hall subgroup of G_i that contains $\varphi_i(H)$; so the set

$$\mathcal{S}_i = \{S \mid \varphi_i(H) \leq S \leq G_i, \text{ S is a } \pi\text{-Hall subgroup of } G_i\}$$

is nonempty. Furthermore, $\varphi_{ij}(\mathcal{S}_i) \subseteq \mathcal{S}_j$. Then $\{\mathcal{S}_i, \varphi_{ij}, I\}$ is an inverse system of nonempty finite sets. Let $(S_i) \in \varprojlim \mathcal{S}_i$; then $\{S_i, \varphi_{ij}\}$ is an inverse system of groups. Finally,

$$H = \varprojlim \varphi_i(H) \leq \varprojlim S_i,$$

and $S = \varprojlim S_i$ is a π-Hall subgroup of G by Lemma 2.3.4.

(c′) Let H and K be π-Hall subgroups of G. Then $\varphi_i(H)$ and $\varphi_i(K)$ are π-Hall subgroups of G_i $(i \in I)$, and so, by assumption, they are conjugate in G_i. Let

$$Q_i = \{q_i \in G_i \mid q_i^{-1}\varphi_i(H)q_i = \varphi_i(K)\}.$$

Clearly $\varphi_{ij}(Q_i) \subseteq Q_j$ $(i \succeq j)$. Therefore, $\{Q_i, \varphi_{ij}\}$ is an inverse system of nonempty finite sets. Using again Proposition 1.1.4, let $q \in \varprojlim Q_i$. Then $q^{-1}Hq = K$, since $\varphi_i(q^{-1}Hq) = \varphi_i(K)$, for each $i \in I$. □

If $\pi = \{p\}$ consists of just one prime, then the Sylow theorems for finite groups (cf. Hall [1959], Theorems 4.2.1–3) guarantee that the assumptions of Theorem 2.3.5 are satisfied for all finite groups. As a consequence we obtain the following generalizations of the Sylow theorems.

Corollary 2.3.6 (The Sylow Theorem for Profinite Groups) *Let G be any profinite group and let p be a fixed prime number. Then*

(a) *G contains a p-Sylow subgroup.*
(b) *Any closed p-subgroup of G is contained in a p-Sylow subgroup.*
(c) *Any two p-Sylow subgroups of G are conjugate.*

Similarly, every finite solvable group C satisfies the assumptions of Theorem 2.3.5 for any set π of prime numbers (cf. Hall [1959], Theorem 9.3.1). Thus one obtains the following result.

Corollary 2.3.7 (The P. Hall Theorem for Prosolvable Groups) *Let G be a prosolvable group, and let π be a fixed set of prime numbers. Then*

(a) *G contains a π-Hall subgroup.*
(b) *Any closed π-subgroup of G is contained in a π-Hall subgroup.*
(c) *Any two π-Hall subgroups of G are conjugate.*

The methods used in Theorem 2.3.5 give an indication of how certain properties valid for the finite groups in a class $\mathcal{C}$, can be generalized to pro-$\mathcal{C}$ groups. The general philosophy is that, if a property is shared by the groups of an inverse system $\{G_i, \varphi_{ij}\}$ of groups, and this property is preserved by the homomorphisms φ_{ij} in some "uniform" manner, then that property will imply a judiciously phrased analogous one for the corresponding inverse limit $\varprojlim G_i$. As further applications of these methods, we mention a few more results that it will be convenient to have explicitly stated for future reference. In most cases we leave the proofs as exercises, although we shall remind the reader of the necessary corresponding properties of finite groups.

If G is a finite nilpotent group, then it has a unique p-Sylow subgroup for each prime p; moreover, G is the direct product of its p-Sylow subgroups. These properties characterize finite nilpotent groups (cf. Hall [1959], Theorem 10.3.4).

Proposition 2.3.8 *A profinite group G is pronilpotent if and only if for each prime number p, G contains a unique p-Sylow subgroup.*

Denote by G_p the unique p-Sylow subgroup of a pronilpotent group G. Then G is the direct product $G = \prod_p G_p$ of its p-Sylow subgroups.

Let G be a prosolvable group. A *Sylow basis* $\{S_p \mid p \text{ a prime number}\}$ for G is a collection of p-Sylow subgroups, one for each prime number p, such that $S_pS_q = S_qS_p$ for each pair of primes p, q. Since Sylow subgroups are compact by definition, S_pS_q is compact, and so closed; hence the last condition implies that S_pS_q is a closed subgroup of G. A theorem of P. Hall asserts that every finite solvable group admits a Sylow basis, and moreover any two such bases are conjugate (cf. Kargapolov and Merzljakov [1979], p. 142). Then, using methods similar to those above, one can prove the following generalization to prosolvable groups.

Proposition 2.3.9 *Let G be a prosolvable group. For each prime number p, let $S_{p'}$ be a p'-Hall subgroup of G. Then*

(a) *For each prime q,*

$$S_q = \bigcap_{p \neq q} S_{p'}$$

is a q-Sylow subgroup of G. The topological closure of the product

$$S_2S_3S_5 \cdots$$

of all the groups S_q is G.

(b) *The collection $\{S_q \mid q\}$ defined in* (a) *is a Sylow basis of G.*

(c) *Any two Sylow bases $\{S_q \mid q\}$ and $\{R_q \mid q\}$ of G are conjugate, that is, there is some $x \in G$ such that $S_q^x = R_q$, for each prime q.*

In a profinite group G of order n, a *p-complement* is a closed subgroup H whose index is p^{n_p}, the highest power of p dividing n. Corollary 2.3.7 asserts that a prosolvable group contains p-complements for every prime p. In the case of finite groups, this property characterizes solvable groups (cf. Hall [1959], Theorem 9.3.3). Correspondingly one has the following

Proposition 2.3.10 *Let G be a profinite group. Then G is prosolvable if and only if G has p-complements for each prime p. If this is the case, a p-complement in G is a p'-Hall subgroup $S_{p'}$ of G, and $G = S_pS_{p'}$, for any p-Sylow subgroup S_p of G.*

Example 2.3.11 The group of p-adic integers $\mathbf{Z}_p$ is naturally embedded in $\widehat{\mathbf{Z}}$, and it is a p-Sylow subgroup of $\widehat{\mathbf{Z}}$. Moreover

$$\widehat{\mathbf{Z}} = \prod_p \mathbf{Z}_p.$$

Note that

$$\#\mathbf{Z}_p = p^\infty, \quad \text{and} \quad \#\widehat{\mathbf{Z}} = \prod_p p^\infty.$$

More generally, if $\mathcal{C}$ is a variety of finite groups, then the pro-$\mathcal{C}$ completion of $\mathbf{Z}$ can be expressed as

$$\mathbf{Z}_{\hat{\mathcal{C}}} = \prod_{C_p \in \mathcal{C}} \mathbf{Z}_p.$$

Exercise 2.3.12

(a) Show that the order of the finite group $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$ is

$$|\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1});$$

(b) For each natural number m, there is a short exact sequence of finite groups

$$I \longrightarrow L_m \longrightarrow \mathrm{GL}_n(\mathbf{Z}/p^m\mathbf{Z}) \xrightarrow{\varphi_m} \mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z}) \longrightarrow I,$$

where I is the $n \times n$ identity matrix, and

$$L_m = \{I + U \mid U \text{ is an } n \times n \text{ matrix with entries in } p(\mathbf{Z}/p^m\mathbf{Z})\};$$

(c) $|\mathrm{GL}_n(\mathbf{Z}/p^m\mathbf{Z})| = p^{(m-1)n^2}(p^n - 1)(p^n - p)\cdots(p^n - p^{n-1})$;

(d) The profinite group $\mathrm{GL}_n(\mathbf{Z}_p)$ has a p-Sylow subgroup of index

$$(p^n - 1)(p^{n-1} - 1)\cdots(p - 1).$$

(Hint: see Exercise 2.1.9.)

Exercise 2.3.13 (The Frattini Argument) Let G be a profinite group and p a prime. Assume H is a closed normal subgroup of G and let P be a p-Sylow subgroup of H. Prove that the normalizer

$$N = N_G(P) = \{x \in G \mid x^{-1}Px = P\}$$

of P in G is closed in G. Moreover, $G = HN$.

Exercise 2.3.14 Let G be a profinite group, $S \leq_c G$ and $W \lhd_c S$. One says that W is *weakly c* (respectively, *strongly c*)* in S with respect to G if for every $g \in G$ with $W^g \leq S$ ones has that $W^g = W$ (respectively, if for every $g \in G$, $W^g \cap S \leq W$).

(a) Let p be a prime number and assume that S is a p-Sylow subgroup of G. Let $\varphi : G \longrightarrow H$ be a continuous epimorphism of profinite groups. Prove that if W is weakly c (respectively, strongly c) in S with respect to G, then $\varphi(W)$ is weakly c (respectively, strongly c) in $\varphi(S)$ with respect to H.
(b) The properties of being weak and strong c are preserved by inverse limits. Explicitly: assume that

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

where $\{G_i, \varphi_{ij}, I\}$ is an inverse system of profinite groups over the poset I. Let $\varphi_i : G \longrightarrow G_i$ $(i \in I)$ be the projection maps. If, for every $i \in I$, $\varphi_i(W)$ is weakly c (respectively, strongly c) in $\varphi_i(S)$ with respect to G_i, then W is weakly c (respectively, strongly c) in S with respect to G.

The following is an analog of the classical Schur-Zassenhaus theorem for finite groups.

Theorem 2.3.15 *Let K be a closed normal Hall subgroup of a profinite group G. Then K has a complement H in G (i.e., H is a closed subgroup of G such that $G = KH$ and $K \cap H = 1$). Moreover, any two complements of K are conjugate in G.*

Proof. Let $\mathcal{U}$ be the collection of all open normal subgroups of G. Let $U \in \mathcal{U}$. Then $K_U = KU/U$ is Hall subgroup of the finite group $G_U = G/U$. Let $\mathcal{S}_U$ the collection of all the complements of K_U in G_U. Then $\mathcal{S}_U \neq \emptyset$ by the theorem of Schur-Zassenhaus for finite groups (cf. Huppert [1967], Theorem I.18.1). If $U, V \in \mathcal{U}$ with $U \leq V$, let $\varphi_{UV} : G_U \longrightarrow G_V$ be the canonical epimorphism. Then $\varphi_{UV}(\mathcal{S}_U) \subseteq \mathcal{S}_V$. Therefore, $\{\mathcal{S}_U \mid U \in \mathcal{U}\}$ is an inverse system of finite nonempty sets. By Proposition 1.1.4,

$$\varprojlim_{U \in \mathcal{U}} \mathcal{S}_U \neq \emptyset.$$

Let $(H_U) \in \varprojlim \mathcal{S}_U$. It follows that the groups $\{H_U \mid U \in \mathcal{U}\}$ form an inverse system (for $U \leq V$, the homomorphism $H_U \longrightarrow H_V$ is the restriction of φ_{UV} to H_U). Define $H = \varprojlim H_U$. It follows that H is a closed subgroup of G such that $\#K$ and $\#H$ are coprime since their images in each G_U are coprime (see Proposition 2.3.2); therefore, $K \cap H = 1$. Finally, note that $G = KH$ by Corollary 1.1.8. Hence H is a complement of K in G.

* The terms 'weakly c' and 'strongly c' correspond to the concepts of 'weakly closed' and 'strongly closed' used in the theory of fusion for finite groups: see Alperin [1967].

Assume that L is another complement of K in G. We have to show that H and L are conjugate in G. Denote by H_U and L_U their corresponding canonical images in G_U. Clearly H_U and L_U are complements of K_U in the finite group G_U. Using again the theorem of Schur-Zassenhaus for finite groups, we deduce that H_U and L_U are conjugate in G_U. For each $U \in \mathcal{U}$, consider the subset E_U of G_U consisting of all elements $e \in G_U$ such that $L_U^e = H_U$. Plainly, $\varphi_{UV}(E_U) \subseteq E_V$ for all pairs $U, V \in \mathcal{U}$ with $U \leq V$. Hence $\{E_U \mid U \in \mathcal{U}\}$ is an inverse system of nonempty sets. By Proposition 1.1.4, there exists some $x = (x_U) \in \varprojlim E_U \subseteq G$. Claim that $L^x = H$. We know that $L_U^{x_U} = H_U$ for every $U \in \mathcal{U}$; hence the claim follows from Corollary 1.1.8. □

Let G be a profinite group and let $K \triangleleft_c G$, $H \leq_c G$ with $G = KH$ and $K \cap H = 1$. As it is usual, we say that G is an internal *semidirect product* of K by H. The standard notation for this situation is $G = K \rtimes H$. (See Example 4.6.2 for the construction of external semidirect products of profinite groups.)

Proposition 2.3.16 *Let $G = K \rtimes H$ be a semidirect product of profinite groups as above. Assume that K is a Hall subgroup of G. Let L be a closed subgroup of K which is normalized by H. If H leaves invariant some coset Lk of L in K, then there exists $x \in Lk$ such that $x^h = x$ for all $h \in H$.*

Proof. The result holds for finite groups (cf. Huppert [1967], Theorem I.18.6). Let $\mathcal{U}$ be the collection of all open normal subgroups of G. For $R \leq_c G$, denote by R_U the image in $G_U = G/U$ of R ($U \in \mathcal{U}$). Note that $|K_U|$ and $|H_U|$ are coprime, and that H_U fixes the coset $L_U k_U$, where k_U is the canonical image of k in K_U. Hence, the set

$$S_U = \{s \in L_U k_U \mid s^{h_U} = s, \text{ for all } h_U \in H_U\}$$

is nonempty (by the result for finite groups). Plainly, the canonical epimorphism $G_U = G/U \longrightarrow G_V = G/V$ ($U \leq V$ in $\mathcal{U}$) maps S_U into S_V. Therefore, $\{S_U \mid U \in \mathcal{U}\}$ is an inverse system of finite nonempty sets. Hence the corresponding inverse limit is not empty (see Proposition 1.1.4). Let

$$x \in \varprojlim_{U \in \mathcal{U}} S_U.$$

Then $x \in Lk$ and $x^h = x$ for all $h \in H$ (see Corollary 1.1.8). □

Exercise 2.3.17 Let G be a profinite group. Define closed subgroups $\gamma_n(G)$ ($n = 1, 2, \dots$) of G as follows

$$\gamma_1(G) = G, \qquad \gamma_{n+1}(G) = \overline{[G, \gamma_n(G)]}.$$

Then $G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G) \geq \cdots$ is called the *lower central series* of G. Prove that the following conditions are equivalent:

(a) G is pronilpotent;
(b)

$$\bigcap_{n=1}^{\infty} \gamma_n(G) = 1.$$

2.4 Generators

Let G be a profinite group and let X be a subset of G. We say that X *generates* G (or, if there could be any danger of confusion, *generates* G *as a profinite group or as a topological group*), if the abstract subgroup $\langle X\rangle$ of G generated by X is dense in G. In that case, we call X a *set of generators* (or, if more emphasis is needed, a *set of topological generators*) of G, and we write $G = \overline{\langle X\rangle}$. We say that a subset X of a profinite group G *converges to* 1 if every open subgroup U of G contains all but a finite number of the elements in X. If X generates G and converges to 1, then we say that X is a *set of generators of* G *converging to* 1. A profinite group is *finitely generated* if it contains a finite subset X that generates G. A profinite group G is called *procyclic* if it contains an element x such that $G = \overline{\langle x\rangle}$. Observe that a profinite group G is procyclic if and only if it is the inverse limit of finite cyclic groups.

Lemma 2.4.1

(a) *Let* $\{G_i, \varphi_{ij}, I\}$ *be a surjective inverse system of profinite groups and let*

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

Denote by $\varphi_i : G \longrightarrow G_i$ $(i \in I)$ *the projection maps. Let* $X \subseteq G$. *Then* X *generates* G *if and only if* $\varphi_i(X)$ *generates* G_i *for each* $i \in I$.

(b) *Let* X *be a subset of a profinite group* G *and let* $\bar{X}$ *denote its closure. Then* X *generates* G *if and only if* $\bar{X}$ *generates* G.

Proof. (a) If X generates G, it is plain that $\varphi_i(X)$ generates G_i for each $i \in I$. Conversely, suppose that $\varphi_i(X)$ generates G_i for each $i \in I$. Put $H = \overline{\langle X\rangle}$. Then $\varphi_i(H) = G_i$ for each $i \in I$. Therefore, $H = G$ by Corollary 1.1.8.

(b) Write $G = \varprojlim G/U$, where U ranges over all the open normal subgroups of G. Then X and $\bar{X}$ have the same image in G/U, for each U. Hence, the result follows from part (a). □

Example 2.4.2 $\widehat{\mathbf{Z}}$ and $\mathbf{Z}_p$ are procyclic groups. If p and q are different prime numbers, then $\mathbf{Z}_p \times \mathbf{Z}_q$ is procyclic. On the other hand, $\mathbf{Z}_p \times \mathbf{Z}_p$ can be generated by two elements, but it is not procyclic.

Exercise 2.4.3 Let X be a set of generators converging to 1 of a profinite group G. Then the topology on $X - \{1\}$ induced from G is the discrete topology. If X is infinite, $\bar{X} = X \cup \{1\}$. If $1 \notin X$ and X is infinite, then $\bar{X}$ is the one-point compactification of X.

Proposition 2.4.4 *Every profinite group G admits a set of generators converging to* 1.

Proof. Consider the set $\mathcal{P}$ of all pairs (N, X_N), where $N \triangleleft_c G$ and $X_N \subseteq G - N$ such that

(i) for every open subgroup U of G containing N, $X_N - U$ is a finite set; and
(ii) $G = \overline{\langle X_N, N \rangle}$.

Note that these two conditions imply that $\tilde{X}_N = \{xN \mid x \in X_N\}$ is a set of generators of G/N converging to 1. Clearly $\mathcal{P} \neq \emptyset$. Define a partial ordering on $\mathcal{P}$ by $(N, X_N) \preceq (M, X_M)$ if $N \geq M$, $X_N \subseteq X_M$ and $X_M - X_N \subseteq N$. We first check that the hypotheses of Zorn's Lemma are met. Let $\{(N_i, X_i) \mid i \in I\}$ be a linearly ordered subset of $\mathcal{P}$; put $K = \bigcap_{i \in I} N_i$ and $X_K = \bigcup_{i \in I} X_i$. We claim that $(K, X_K) \in \mathcal{P}$. Clearly $X_K \subseteq G - K$. Observe that for each $i \in I$, the natural epimorphism $\varphi_i : G/K \longrightarrow G/N_i$ sends $\tilde{X}_K$ onto $\tilde{X}_i$. By Lemma 2.4.1, $\tilde{X}_K$ generates $G/K = \varprojlim_{i \in I} G/N_i$. Hence condition (ii) holds. Finally, we check condition (i). Let $K \leq U \triangleleft_o G$; then (see Proposition 2.1.5), there is some $i_0 \in I$ such that $U \geq N_{i_0}$. So, $X_K - U = X_{i_0} - U$. Therefore, $X_K - U$ is finite. This proves the claim. One easily verifies that (K, X_K) is an upper bound for the chain $\{(N_i, X_i) \mid i \in I\}$; hence $(\mathcal{P}, \preceq)$ is an inductive poset. By Zorn's Lemma, there exists a maximal pair (M, X) in $\mathcal{P}$. To finish the proof, it suffices to show that $M = 1$. Assuming otherwise, let $U \triangleleft_o G$ be such that $U \cap M$ is a proper subgroup of M. Choose a finite subset T of $M - (U \cap M)$ such that $M = \langle T, U \cap M \rangle$. Clearly, $(U \cap M, X \cup T) \in \mathcal{P}$. Furthermore, $(M, X) \prec (U \cap M, X \cup T)$. This contradicts the maximality of (M, X). Thus $M = 1$. □

Definition 2.4.5 *Let G be a profinite group. Define $d(G)$ to be the smallest cardinality of a set of generators of G converging to* 1.

We now consider the question of what types of closed subsets X of a profinite group G can generate G, as an abstract group. This is obviously the case if $X = G$; we shall see that, in some sense, one can deviate very little from this case. Denote by $\mathrm{Pr}_n(X)$ the set of all finite products of the form $x_1^{\pm 1} \cdots x_n^{\pm 1}$, where $x_1, \ldots, x_n \in X$. Then we have the following result, which is valid in fact for any compact Hausdorff topological group G.

Lemma 2.4.6 *Let G be a profinite group and let X be a closed subset of G such that $X = X^{-1}$ and $1 \in X$. Then $G = \langle X \rangle$ (generated as an abstract group) if and only if $G = \mathrm{Pr}_m(X)$ for some $m = 1, 2, \ldots$.*

Proof. It is plain that if $G = \mathrm{Pr}_m(X)$, then $G = \langle X \rangle$. Conversely, suppose that $G = \langle X \rangle$. By assumption $G = \bigcup_{n=1}^{\infty} \mathrm{Pr}_n(X)$, and clearly each $\mathrm{Pr}_n(X)$ is closed. By Proposition 2.3.1, a profinite group cannot be the union of countably many closed subsets with empty interior. Hence $\mathrm{Pr}_t(X)$ contains a nonempty open set U for some $t = 1, 2, \ldots$. Clearly $G = \bigcup_{g \in G} gU$. By compactness there exist finitely many $g_1, \ldots, g_r \in G$ such that $G = \bigcup_{i=1}^{r} g_i U$. Since $G = \langle X \rangle$, there exists some s such that $g_1, \ldots, g_r \in Pr_s(X)$. Put $m = t + s$; then $G = \mathrm{Pr}_m(X)$. □

2.5 Finitely Generated Profinite Groups

A closed subgroup K of a profinite group is called *characteristic* if $\varphi(K) = K$ for all continuous automorphisms φ of G.

Proposition 2.5.1 *Let G be a finitely generated profinite group.*

(a) *For each natural number n, the number of open subgroups of G of index n is finite.*
(b) *The identity element 1 of G has a fundamental system of neighborhoods consisting of a countable chain of open characteristic subgroups*

$$G = V_0 \geq V_1 \geq V_2 \geq \cdots.$$

Proof. (a) If H is an open subgroup of G, the number of conjugates $H^g = g^{-1}Hg$ of H in G is finite, since H has finite index in G. Hence the core $H_G = \bigcap_{g \in G} H^g$ of H in G has finite index in G; so H_G is open in G. Consequently it suffices to show that G has finitely many open normal subgroups N of index m, for a fixed natural number m. But such a group N is the kernel of an epimorphism $\varphi : G \longrightarrow R$, for some finite group R of order m. Observe that such φ is completely determined by its values on a given finite set of generators of G. Therefore, for a fixed R there are only finitely many epimorphisms φ. On the other hand, there are only finitely many groups of order m. Thus there are finitely many such N.

(b) Let n be a natural number. Define V_n to be the intersection of all open subgroups of G of index at most n. By (a), V_n is open and characteristic. It is obvious that $V_n \geq V_{n+1}$ for all natural numbers n. These subgroups form a fundamental system of neighborhoods of 1 since every open subgroup contains some V_n. □

A group G is *Hopfian* if every endomorphism of G which is onto is an isomorphism. Next we establish an analog of the Hopfian property for profinite groups.

Proposition 2.5.2 *Let G be a finitely generated profinite group and let $\varphi : G \longrightarrow G$ be a continuous epimorphism. Then φ is an isomorphism.*

Proof. We claim that φ is an injection. To see this, it is enough to show that $\mathrm{Ker}(\varphi)$ is contained in every open normal subgroup of G. For each natural number n denote by $\mathcal{U}_n$ the set of all open normal subgroups of G of index n. By Proposition 2.5.1 $\mathcal{U}_n$ is finite. Define

$$\Phi : \mathcal{U}_n \longrightarrow \mathcal{U}_n$$

to be the function given by $\Phi(U) = \varphi^{-1}(U)$. Clearly Φ is injective. Since $\mathcal{U}_n$ is finite, Φ is bijective. Let U be an open normal subgroup of G; then U has finite index, say n, in G. Therefore $U = \varphi^{-1}(V)$ for some open normal subgroup V, and thus $U \geq \mathrm{Ker}(\varphi)$, as desired. Hence φ is an injection. Thus φ is a bijection. Since G is compact, it follows that φ is a homeomorphism, and so an isomorphism of profinite groups. □

Lemma 2.5.3 *Let $\{G_i, \varphi_{ij}, I\}$ be a surjective inverse system of finite groups. Define*

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

Then $d(G) < \infty$ if and only if $\{d(G_i) \mid i \in I\}$ is a bounded set; in this case, there exists some $i_o \in I$ such that $d(G) = d(G_j)$, for each $j \geq i_o$.

Proof. Let $d(G) = n < \infty$. Since the projection $\varphi_i : G \longrightarrow G_i$ is an epimorphism (see Proposition 1.1.10), we have that $d(G_i) \leq n$ for each $i \in I$. Conversely, assume $n < \infty$ is the least upper bound of $\{d(G_i) \mid i \in I\}$; say $n = d(G_{i_o})$. For each $i \in I$, let $\mathcal{X}_i$ be the set of all n-tuples $(x_1, \ldots, x_n) \in G_i \times \cdots \times G_i$ such that $\overline{\langle x_1, \ldots, x_n\rangle} = G_i$. Then clearly $\{\mathcal{X}_i, \varphi_{ij}, I\}$ is in a natural way an inverse system of nonempty sets. By Proposition 1.1.4, $\varprojlim \mathcal{X}_i \neq \emptyset$. Let $Y = (y_1, \ldots, y_n) \in \varprojlim \mathcal{X}_i$. It follows from Corollary 1.1.8 that $G = \overline{\langle y_1, \ldots, y_n\rangle}$. Finally, it is plain that if $j \geq i_o$, then $d(G) = d(G_j)$. □

Proposition 2.5.4 *Let G and H be finitely generated profinite groups and let n be a natural number with $d(G) \leq n$. Let*

$$\varphi : G \longrightarrow H$$

be a continuous epimorphism and assume that $H = \overline{\langle h_1, \ldots, h_n\rangle}$. Then there exist $g_1, \ldots, g_n \in G$ such that $G = \overline{\langle g_1, \ldots, g_n\rangle}$ and $\varphi(g_i) = h_i$ $(i = 1, \ldots, n)$.

Proof.

Case 1. G is finite.

For $\mathbf{h} = (h_1, \ldots, h_n) \in H \times \cdots \times H$ with $\langle h_1, \ldots, h_n\rangle = H$, let $t_G(\mathbf{h})$ denote the number of n-tuples

$$\mathbf{g} = (g_1, \ldots, g_n) \in G \times \cdots \times G$$

such that $\langle g_1, \dots, g_n \rangle = G$ and $\varphi(g_i) = h_i$ for all i. Let $\mathbf{g} = (g_1, \dots, g_n) \in G \times \cdots \times G$ be a tuple such that $\varphi(g_i) = h_i$ for all i; then any tuple $\mathbf{g}' = (g_1', \dots, g_n')$ with $\varphi(g_i') = h_i$ $(i = 1, \dots, n)$ must be in

$$g_1\mathrm{Ker}(\varphi) \times \cdots \times g_n\mathrm{Ker}(\varphi).$$

Hence

$$t_G(\mathbf{h}) = |\mathrm{Ker}(\varphi)|^n - \sum t_L(\mathbf{h}),$$

where the sum is taken over the collection of proper subgroups L of G for which $\varphi(L) = H$.

We have to show that $t_G(\mathbf{h}) \geq 1$. This is certainly the case for certain types of tuples $\mathbf{h}$, for example, take $\mathbf{h} = \varphi(\mathbf{g})$, where $\mathbf{g} = (g_1, \dots, g_n)$ and $g_1, \dots, g_n$ is a set of generators of G. Therefore the result follows if we prove the following assertion: $t_G(\mathbf{h})$ is independent of $\mathbf{h}$. Observe that this assertion holds if G does not contain any proper subgroup L with $\varphi(L) = H$, since in this case $t_G(\mathbf{h})$ is precisely the total number of n-tuples $\mathbf{g} \in G \times \cdots \times G$ such that $\varphi(\mathbf{g}) = \mathbf{h}$, namely $|\mathrm{Ker}(\varphi)|^n$. We prove the assertion by induction on $|G|$. Assume that it holds for all epimorphisms $L \longrightarrow H$ such that $|L| < |G|$. Then the above formula shows that $t_G(\mathbf{h})$ is independent of $\mathbf{h}$.

Case 2. G is infinite.

Let $\mathcal{U}$ be the collection of all open normal subgroups of G. For each $U \in \mathcal{U}$ consider the natural epimorphism $\varphi_U : G/U \longrightarrow H/\varphi(U)$ induced by φ. Then

$$\varphi = \varprojlim_{U \in \mathcal{U}} \varphi_U.$$

For $h \in H$, denote by h^U its natural image in $H/\varphi(U)$. Plainly $H/\varphi(U) = \langle h_1^U, \dots, h_n^U \rangle$. Let $\mathcal{X}_U$ be the set of all n-tuples $(y_1, \dots, y_n) \in G/U \times \cdots \times G/U$ such that $\langle y_1, \dots, y_n \rangle = G/U$ and $\varphi(y_i) = h_i^U$ $(i = 1, \dots, n)$. By Case 1, $\mathcal{X}_U \neq \emptyset$. Clearly the collection $\{\mathcal{X}_U \mid U \in \mathcal{U}\}$ is an inverse system of sets in a natural way. It follows then from Proposition 1.1.4 that there exists some

$$(g_1, \dots, g_n) \in \varprojlim_{U \in \mathcal{U}} \mathcal{X}_U \subseteq G \times \cdots \times G.$$

Then it is immediate that $\varphi(g_i) = h_i$ $(i = 1, \dots, n)$ and $G = \overline{\langle g_1, \dots, g_n \rangle}$. □

Finite generation is a property preserved by open subgroups as we show in the next proposition (we shall give a more precise result later on in Corollary 3.6.3).

Proposition 2.5.5 *Let G be a finitely generated profinite group and let U be an open subgroup of G. Then U is also finitely generated.*

Proof. Let X be a finite set of generators of G and let T be a right transversal of U in G such that $1 \in T$. Replacing X by $X \cup X^{-1}$ if necessary, we may assume that $X = X^{-1}$. If $g \in G$, denote by $\tilde{g}$ the element of T such that $Ug = U\tilde{g}$. Define

$$Y = \{tx(\widetilde{tx})^{-1} \mid x \in X, t \in T\}.$$

Then Y is a finite set since both X and T are finite sets. We claim that $\overline{\langle Y \rangle} = U$. Put $H = \overline{\langle Y \rangle}$. Plainly $Y \subseteq U$, and so $H \leq U$. Let $h \in H$; then, for $t \in T$ and $x \in X$, we have $htx = htx(\widetilde{tx})^{-1}\widetilde{tx} \in HT$. Since $1 \in HT$, this shows that $X \subseteq HTX \subseteq HT$, and so $X^k \subseteq HT$ for $k = 0, 1, 2, \ldots$. Hence $\langle X \rangle \leq HT$, because $X = X^{-1}$. Since T is finite, HT is closed, so $HT = G$. We deduce that the index of H in G is at most $|T| = [G : U]$. Since $H \leq U$, it follows that $H = U$ (see Proposition 2.3.2). □

2.6 Generators and Chains of Subgroups

Let X be a topological space. Define the *weight* $w(X)$ of X to be the smallest cardinal of a base of open sets of X. We denote by $\rho(X)$ the cardinal of the set of all clopen subsets of X. If G is a topological group, its *local weight* $w_0(G)$ is defined as the smallest cardinal of a fundamental system of open neighborhoods of 1 in G. When G is an infinite profinite group, it follows from Theorem 2.1.3 that $w_0(G)$ is the cardinal of any fundamental system of neighborhoods of 1 consisting of open subgroups. Note that for a profinite group G, $w_0(G)$ is finite only if G is finite; and in that case $w_0(G) = 1$. More generally, if H is a closed subgroup of G, we define the local weight of G/H to be the smallest cardinal of a fundamental system of open neighborhoods of a point of G/H. Since for any two points of the quotient space G/H, there is a homeomorphism of G/H that maps one of those points to the other, this definition is independent of the point used.

Proposition 2.6.1

(a) *Let X be an infinite profinite space. Then $w(X) = \rho(X)$. In particular, the cardinality of any base of open sets of X consisting of clopen sets is $\rho(X)$.*
(b) *If G is an infinite profinite group, then $w_0(G) = w(G) = \rho(G)$.*

Proof. (a) By Theorem 1.1.12, $w(X) \leq \rho(X)$. Let $\mathcal{U}$ be a base of open sets of X such that $|\mathcal{U}| = w(X)$. For each clopen set W in X, choose a finite subset $\Phi(W)$ of $\mathcal{U}$ such that W is the union of the sets in $\Phi(W)$. It follows that Φ is an injective function from the set of all clopen subsets to the set of finite subsets of $\mathcal{U}$. Hence, $w(X) \geq \rho(X)$.

(b) Let $\mathcal{N}$ be a fundamental system of neighborhoods of 1 consisting of open normal subgroups. Then $\{gN \mid N \in \mathcal{N}\}$ is a base of open sets of G. The cardinality of this base is still $w_0(G)$ since each $N \in \mathcal{N}$ has finite index in G. So $w_0(G) \geq w(G)$, and therefore $w_0(G) = w(G)$. By part (a), the result follows. □

Proposition 2.6.2 *Let G be an infinite profinite group.*

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

Proof. (a) By Theorem 2.1.3, $w_0(G)$ is the cardinal of the set of open normal subgroups of G. Observe that an open normal subgroup arises always as the kernel of a continuous homomorphism from G onto a finite group. If H is a finite group, a continuous homomorphism

$$\varphi : G \longrightarrow H$$

is completely determined by its restriction to X; and a continuous mapping from X to H is determined by its values on at most $|H|$ clopen subsets of X. Therefore, there are at most $\rho(X)$ continuous homomorphisms from G to H. Since X is infinite and there are countably many nonisomorphic finite groups, it follows that there are at most $\rho(X)$ continuous homomorphisms from G to a finite group. Thus, there exist at most $\rho(X)$ open normal subgroups in G. So $w_0(G) \leq \rho(X)$. On the other hand, $\rho(X) \leq \rho(G)$ since $X \leq G$. Finally, it follows from Proposition 2.6.1 that $\rho(G) = w_0(G)$.

(b) The set $\bar{X} = X \cup \{1\}$ is the one-point compactification of $X - \{1\}$ (see Exercise 2.4.3). Hence a base of open sets of $\bar{X}$ consists of the subsets of $X - \{1\}$ and the complements in $\bar{X}$ of the finite subsets of $X - \{1\}$. Hence the clopen subsets of $\bar{X}$ are the finite subsets of $X - \{1\}$ and their complements in $\bar{X}$. Therefore $\rho(\bar{X}) = |X|$.Thus the result follows from (a). □

As a consequence of the above proposition and the definition of $d(G)$ (see Definition 2.4.5), one has

Corollary 2.6.3 *Let G be a profinite group. If $d(G)$ is infinite, then $d(G) = w_0(G)$.*

Theorem 2.6.4 *Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups. Assume that G is a pro-$\mathcal{C}$ group. Let μ be an ordinal number, and let $|\mu|$ denote its cardinal. Then $w_0(G) \leq |\mu|$ if and only if there exists a chain of closed normal subgroups G_λ of G, indexed by the ordinals $\lambda \leq \mu$*

$$G = G_0 \geq G_1 \geq \cdots \geq G_\lambda \geq \cdots \geq G_\mu = 1 \tag{3}$$

such that

(a) *$G_\lambda / G_{\lambda+1}$ is a group in $\mathcal{C}$;*
(b) *if λ is a limit ordinal, then $G_\lambda = \bigcap_{\nu<\lambda} G_\nu$.*

Moreover, if G is infinite, μ and the chain (3) can be chosen in such a way that

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

Proof. If G is finite, the result is obvious. So, let G be infinite. Assume that μ is the smallest ordinal whose cardinal is $w_0(G)$. Let $\{U_\lambda \mid \lambda < \mu\}$ be a fundamental system of open neighborhoods of 1 consisting of open normal subgroups of G, indexed by the ordinals less that μ. For each $\lambda \le \mu$, let $G_\lambda = \bigcap_{\nu<\lambda} U_\nu$. Then G/G_λ is pro-$\mathcal{C}$ (see Proposition 2.2.1), and clearly (a) and (b) hold. To check (c), assume $\lambda < \mu$; observe that

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

is a fundamental system of open normal subgroups of G/G_λ. Therefore,

$$w_0(G/G_\lambda) \le |\lambda| < |\mu| = w_0(G).$$

Conversely, suppose that there is a chain (3) of closed normal subgroups satisfying conditions (a) and (b). We shall show by transfinite induction on λ that for each $\lambda \le \mu$, $w_0(G/G_\lambda) \le |\lambda|$. This is obviously true if $\lambda = 1$. Suppose the statement holds for all ordinals $\nu < \lambda$. If λ is a nonlimit ordinal, then $\lambda = \lambda' + 1$, for some λ'. Since $[G_{\lambda'} : G_\lambda]$ is finite, there is some $V \triangleleft_o G$ such that $G_\lambda = V \cap G_{\lambda'}$. By the induction hypothesis there is a collection $\mathcal{U}'$ of open normal subgroups of G containing $G_{\lambda'}$ such that $\{U/G_{\lambda'} \mid U \in \mathcal{U}'\}$ is a fundamental system of open neighborhoods of the identity in $G/G_{\lambda'}$ and $|\mathcal{U}'| \le |\lambda'|$. Let $\mathcal{U} = \{V \cap U' \mid U' \in \mathcal{U}'\}$. Then $\bigcap_{U\in\mathcal{U}} U = G_\lambda$. Obviously $|\mathcal{U}| \le |\lambda|$, and it is easily checked that $\{U/G_\lambda \mid U \in \mathcal{U}\}$ is a fundamental system of open neighborhoods of the identity in G/G_λ (see Proposition 2.1.5); therefore $w_0(G/G_\lambda) \le |\lambda|$. Suppose now that λ is a limit ordinal. By hypothesis, if $\nu < \lambda$, then there exists a set $\mathcal{U}_\nu$ of open subgroups of G containing G_ν such that $\{U/G_\nu \mid U \in \mathcal{U}_\nu\}$ is a fundamental system of open neighborhoods of the identity in G/G_ν and $|\mathcal{U}_\nu| \le |\nu|$. Put $\mathcal{U}_\lambda = \bigcup_{\nu<\lambda} \mathcal{U}_\nu$. Then $\bigcap_{U\in\mathcal{U}_\lambda} U = G_\lambda$; hence, the set $\mathcal{U}$ of finite intersections of groups in $\mathcal{U}_\lambda$ form a fundamental system of open neighborhoods of the identity in G/G_λ (see Proposition 2.1.5). Furthermore,

$$|\mathcal{U}| = |\mathcal{U}_\lambda| \le \sum_{\nu<\lambda} |\mathcal{U}_\nu| \le |\lambda|,$$

since λ is infinite. □

The next result is partly a consequence of the theorem above and partly a refinement of it.

Corollary 2.6.5 *Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups. Assume that G is a pro-$\mathcal{C}$ group and let H be a closed* *normal subgroup of* G*. Then there exists an ordinal number* μ *and a chain of closed pro-*$\mathcal{C}$ *subgroups* H_λ *of* H

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

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

(a) $H_\lambda \triangleleft G$ *and* $H_\lambda/H_{\lambda+1} \in \mathcal{C}$*, for each* $\lambda < \mu$;
(b) *Either* $H_{\lambda+1} = H_\lambda$ *or the group* $H_{\lambda+1}$ *is a maximal subgroup of* H_λ *with respect to property* (a);
(c) *If* λ *is a limit ordinal, then* $H_\lambda = \bigcap_{\nu<\lambda} H_\nu$;
(d) *If either* H *or* G/H *is an infinite group, then*

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

(e) *Assume that* H *is infinite. Let* M *be a closed normal subgroup of* G *containing* H*. If* $w_0(M/H) < w_0(G)$*, then* $w_0(M/H_\lambda) < w_0(G)$ *whenever* $\lambda < \mu$*.*

Proof. If H is finite, the result follows from Theorem 2.6.4: using the notation of that theorem, denote the (finite!) collection of subgroups $\{H \cap G_\lambda \mid \lambda \leq \mu\}$ of H by $\{H_0', H_1', \ldots, H_t'\}$, where $H = H_0' \geq H_1' \geq \cdots \geq H_t' = 1$. Then condition (a) holds for this collection; if (b) fails, one can easily add to this collection finitely many subgroups so that the new collection satisfies (a) and (b).

Assume that H is infinite. Let $\mathcal{U}$ be the set of all open normal subgroups of G. The collection $\mathcal{U}(H) = \{U \cap H \mid U \in \mathcal{U}\}$ is a fundamental system of open neighborhoods of 1 in H. The cardinality of this collection is $w_0(H)$. Let μ be the smallest ordinal whose cardinality is $|\mathcal{U}(H)|$. Index the distinct elements of $\mathcal{U}(H)$ by the ordinals less than μ, say $\{U_\lambda \mid \lambda < \mu\}$. For each $\lambda \leq \mu$, let $H_\lambda = \bigcap_{\nu<\lambda} U_\nu$. Then H_λ is normal in G, and so it is pro-$\mathcal{C}$ (see Proposition 2.2.1). Clearly (a) and (c) are satisfied. Adding finitely many subgroups between $H_{\lambda+1}$ and H_λ if necessary, we may assume that (b) holds. Next we prove (d). By Theorem 2.6.4 and the above, there exists a chain

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

of closed normal subgroups of G satisfying conditions (a) and (b) of Theorem 2.6.4; hence $w_0(G) \leq w_0(H) + w_0(G/H)$. Now, note that

$$\{U/H \mid U \in \mathcal{U}, U \geq H\}$$

is a fundamental system of open neighborhoods of 1 in G/H and

$$\{H \cap U \mid U \in \mathcal{U}, U \not\geq H\}$$

is a fundamental system of open neighborhoods of 1 in H. Hence $w_0(G) \geq w_0(H)+w_0(G/H)$. Thus $w_0(G) = w_0(H)+w_0(G/H)$. Part (e) is proved as in the theorem: assume $\lambda < \mu$; observe that $\{U_\nu/H_\lambda \mid \nu < \lambda\}$ is a fundamental system of open normal subgroups of H/H_λ. Therefore, $w_0(H/H_\lambda) \leq |\lambda| < |\mu| = w_0(G)$, where if ρ is an ordinal, then $|\rho|$ denotes its cardinality. Thus, $w_0(M/H_\lambda) \leq w_0(M/H) + w_0(H_\lambda/H) < w_0(G)$. □

Corollary 2.6.6 *Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups. Let G be a profinite group and let X be a system of generators converging to* 1*. Then $|X| \leq \aleph_0$ if and only if G admits a countable descending chain of open normal subgroups*

$$G = G_0 \geq G_1 \geq \cdots \geq G_i \geq \cdots$$

such that $\bigcap_{i=0}^{\infty} G_i = 1$, that is, if and only if the identity element 1 *of G admits a fundamental system of neighborhoods consisting of a countable chain of open subgroups.*

Proof. If $|X|$ is infinite, then the result is a consequence of Proposition 2.6.2 and Theorem 2.6.4. If $|X|$ is finite this follows from Proposition 2.5.1. □

Remark 2.6.7 It is known that a topological group G is metrizable if and only if the identity element of G admits a countable fundamental system of neighborhoods (cf. Hewitt and Ross [1963], Theorem 8.3). So, according to the corollary above, a profinite group is metrizable if and only if it has a finite or a countably infinite set of generators converging to 1.

2.7 Procyclic Groups

Recall that a procyclic group is an inverse limit of finite cyclic groups, or equivalently (see Lemma 2.5.3), a procyclic group is a profinite group that can be generated by one element. As with finite cyclic groups it is very simple to classify such groups in terms of their orders.

Proposition 2.7.1 *Let p be a prime number and p^n a supernatural number* $(0 \leq n \leq \infty)$.

(a) *There exists a unique procyclic group C of order p^n up to isomorphism*; *namely, if $n < \infty$, $C \cong \mathbf{Z}/p^n\mathbf{Z}$, and if $n = \infty$, $C \cong \mathbf{Z}_p$.*
(b) *The group $\mathbf{Z}_p$ has a unique closed subgroup H of index p^n. Moreover, $H = p^n\mathbf{Z}_p \cong \mathbf{Z}_p$ if n is finite, and $H = 1$ if n is infinite.*
(c) *Every procyclic group of order p^n appears as a quotient of $\mathbf{Z}_p$ in a unique way.*
(d) *$\mathbf{Z}_p$ cannot be written as a direct product of nontrivial subgroups.*

Proof. Let C be a procyclic group of order p^∞, and let U and V be open subgroups of C with the same indexes; then $U/U \cap V$ and $V/U \cap V$ are subgroups of the finite cyclic group $C/U \cap V$ with the same index, and so

$U = V$. It follows that for each natural number i, the group C has a unique open subgroup U_i of index p^i. Therefore,

$$C \cong \varprojlim_i C/U_i \cong \varprojlim_i \mathbf{Z}/p^i\mathbf{Z} \cong \mathbf{Z}_p.$$

This proves (a). The above argument shows that $\mathbf{Z}_p$ has a unique closed subgroup H of index p^n if n is finite; so it must coincide with $p^n\mathbf{Z}_p$. Furthermore, in this case $\#H = p^\infty$ by Proposition 2.3.2 and therefore $H \cong \mathbf{Z}_p$ as shown in (a). To finish the proof of (b), assume that H is a closed subgroup of $\mathbf{Z}_p$ of index p^∞. Put $U_i = p^i\mathbf{Z}_p$ $(i = 1, 2, \ldots)$. Then, by the definition of index, for each $i \in \mathbf{N}$ there is some $j \in \mathbf{N}$ such that $U_jH \le U_i$; therefore,

$$H = \bigcap_{i=1}^{\infty} U_iH = 1.$$

Statement (c) follows from (b).

To prove (d) observe that if A and B are nontrivial subgroups of $\mathbf{Z}_p$, then they have finite index and hence so does their intersection. Thus $A \cap B \cong \mathbf{Z}_p$ according to (a). Therefore $\mathbf{Z}_p \ncong A \times B$. □

If G is a procyclic group then it is the direct product $G = \prod_p G_p$ of its p-Sylow subgroups (see Proposition 2.3.8). Clearly each G_p is a pro-p procyclic group. In particular, $\widehat{\mathbf{Z}} = \prod_p \mathbf{Z}_p$. Conversely, the direct product $G = \prod_p H(p)$ of pro-p procyclic groups $H(p)$, where p runs through different primes, is a procyclic group; indeed, if U is an open subgroup of G, then G/U is a finite cyclic group. These facts together with the proposition above yield the following description for general procyclic groups.

Theorem 2.7.2 *Let $n = \prod_p p^{n(p)}$ be a supernatural number.*

(a) *There exists a unique procyclic group C of order n up to isomorphism.*
(b) *The group $\widehat{\mathbf{Z}}$ has a unique closed subgroup H of index n. Moreover,*

$$H \cong \prod_{p \in S} \mathbf{Z}_p,$$

where $S = \{p \mid n(p) < \infty\}$.
(c) *Every procyclic group of order n is a quotient of $\widehat{\mathbf{Z}}$ in a unique way.*

2.8 The Frattini Subgroup of a Profinite Group

Let G be a profinite group. According to Proposition 2.1.4, every closed subgroup of G is the intersection of open subgroups; hence a maximal closed subgroup of G is necessarily open. Moreover, if G is nontrivial, it always has maximal open subgroups. Define the *Frattini subgroup* $\Phi(G)$ of G to be the intersection of all its maximal open subgroups. Observe that, unlike what could happen for abstract infinite groups, if G is a nontrivial profinite group, then one always has $\Phi(G) < G$. Plainly $\Phi(G)$ is a characteristic subgroup of G, that is, for every continuous automorphism ψ of G, $\psi(\Phi(G)) = \Phi(G)$. The quotient group $G/\Phi(G)$ is called the *Frattini quotient* of G.

An element g of profinite group G is a *nongenerator* if it can be omitted from every generating set of G, that is, whenever $G = \overline{\langle X, g\rangle}$, then $G = \overline{\langle X\rangle}$.

Lemma 2.8.1 *The Frattini subgroup $\Phi(G)$ of a profinite group G coincides with the set S of all nongenerators of G.*

Proof. Let $g \in S$. If H is a maximal open subgroup of G and $g \notin H$, then $G = \overline{\langle H, g\rangle}$ but $G \neq H$; this is a contradiction since g is a nongenerator. Thus there is no such maximal subgroup H, and so $g \in \Phi(G)$.

Now, let $g \in \Phi(G)$; we must show that $g \in S$. Assume on the contrary that $g \notin S$, that is, assume that there exists a subset X of G such that $G = \overline{\langle X, g\rangle}$, but $G \neq \overline{\langle X\rangle}$. Observe that

$$\overline{\langle X, g\rangle} = \overline{\langle \overline{\langle X\rangle}, g\rangle}.$$

Since $\overline{\langle X\rangle}$ is the intersection of the open subgroups of G containing $\overline{\langle X\rangle}$ (see Proposition 2.1.4), there exists an open subgroup H of G maximal with respect to the properties of containing $\overline{\langle X\rangle}$ and not containing g. Remark that H is in fact a maximal open subgroup of G; indeed, if $H < K \leq_o G$, then $K \geq \langle X, g\rangle$ and so $K = G$. Since $g \notin H$, we have $g \notin \Phi(G)$, a contradiction. Therefore, $g \in S$ as needed. □

Proposition 2.8.2

(a) *Let G be a profinite group. If $N \triangleleft_c G$ and $N \leq \Phi(G)$, then $\Phi(G/N) = \Phi(G)/N$.*
(b) *If $\rho : G \longrightarrow H$ is an epimorphism of profinite groups, then $\rho(\Phi(G)) \leq \Phi(H)$.*
(c) *If $\{G_i, \varphi_{ij}, I\}$ is a surjective inverse system of profinite groups over the directed indexing set I, then*

$$\Phi\Big(\varprojlim_{i\in I} G_i\Big) = \varprojlim_{i\in I} \Phi(G_i).$$

Proof. Part (a) follows immediately from the definition. Part (b) is clear since $\rho^{-1}(M)$ is a maximal subgroup of G whenever M is a maximal subgroup of H.

(c) Put $G = \varprojlim_{i\in I} G_i$, and note that the canonical projection

$$\varphi_i : G \longrightarrow G_i$$

is an epimorphism (see Proposition 1.1.10). By (b), $\varphi_i(\Phi(G)) \leq \Phi(G_i)$, for every $i \in I$. Hence

$$\Phi(G) = \varprojlim_{i\in I} \varphi_i(\Phi(G)) \le \varprojlim_{i\in I} \Phi(G_i).$$

Consider now an element

$$x = (x_i) \in \varprojlim_{i\in I} \Phi(G_i),$$

and suppose $x \notin \Phi(G)$. Then there is a maximal open subgroup M of G with $x \notin M$. Hence, $x_i \notin \varphi_i(M)$ for some $i \in I$. Since $\varphi_i(M)$ is a maximal subgroup of G_i, one has that $x_i \notin \Phi(G_i)$, a contradiction. Therefore $x \in \Phi(G)$, and so

$$\varprojlim_{i\in I} \Phi(G_i) \le \Phi(G).$$

□

Corollary 2.8.3 *If G is a profinite group, then*

$$G/\Phi(G) = \varprojlim_{U} (G/U)/\Phi(G/U),$$

where U runs through the open normal subgroups of G.

Proof. Consider the short exact sequence

$$1 \longrightarrow \Phi(G/U) \longrightarrow G/U \longrightarrow (G/U)/\Phi(G/U) \longrightarrow 1,$$

apply (the exact functor) $\varprojlim$, and use Proposition 2.8.2. □

Corollary 2.8.4 *If G is a profinite group, then $\Phi(G)$ is pronilpotent.*

Proof. This follows from Proposition 2.8.2 and the corresponding result for finite groups (cf. Hall [1959], Theorem 10.4.2). □

Corollary 2.8.5 *Let G be a profinite group, $H \le_c G$ and $Y \subseteq \Phi(G)$. Assume that $G = \overline{\langle H, Y\rangle}$. Then $G = H$. In particular, if $H\Phi(G) = G$, then $H = G$.*

Proof. Express G as

$$G = \varprojlim_{U} G/U,$$

where U runs through the open normal subgroups of G. By Proposition 2.8.2, $YU/U \subseteq \Phi(G/U)$. Then, using Lemma 2.8.1,

$$G = \varprojlim_{U} \langle HU/U, YU/U\rangle = \varprojlim_{U} HU/U = H.$$

□

Lemma 2.8.6 *Let G be a finitely generated profinite group. Then $d(G) = d(G/\Phi(G))$.*

Proof. Obviously $d(G) \geq d(G/\Phi(G))$. Consider the canonical epimorphism $\psi : G \longrightarrow G/\Phi(G)$. Let $X \subseteq G$ be such that $\psi(X)$ is a minimal set of generators of $G/\Phi(G)$. Then $G = \overline{\langle X, \Phi(G)\rangle} = \overline{\langle X\rangle}\Phi(G) = \overline{\langle X\rangle}$ by Corollary 2.8.5; so $d(G/\Phi(G)) \geq d(G)$. □

For a pro-p group G the properties of its Frattini subgroup are particularly useful. We begin with the following lemma. As usual, if H, K are subgroups of a group G, we denote by $[H, K]$ the subgroup of G generated by the *commutators* $[h, k] = h^{-1}k^{-1}hk$ $(h \in H, k \in K)$.

Lemma 2.8.7 *Let p be a prime number and let G be a pro-p group.*

(a) *Every maximal closed subgroup M of G has index p.*
(b) *The Frattini quotient $G/\Phi(G)$ is a p-elementary abelian profinite group, and hence a vector space over the field $\mathbf{F}_p$ with p elements.*
(c) *$\Phi(G) = \overline{G^p[G, G]}$, where $G^p = \{x^p \mid x \in G\}$ and $[G, G]$ denotes the commutator subgroup of G.*

Proof. (a) Let $M_G = \bigcap_{g\in G} M^g$ be the core of M in G. Then M/M_G is a maximal subgroup of the finite p-group G/M_G and so normal of index p (cf. Hall [1959], Theorem 4.3.2). Deduce that M is normal of index p in G.

(b)
$$G/\Phi(G) = G/\bigcap M \hookrightarrow \prod G/M,$$
where M runs through the closed maximal subgroups of G. By (a) $G/M \cong \mathbf{Z}/p\mathbf{Z}$ for each M, so the result follows.

(c) Put $G_0 = \overline{G^p[G, G]}$. Since the Frattini quotient $G/\Phi(G)$ is elementary abelian, one has $\Phi(G) \geq G_0$. To see that these two groups are in fact the same, consider an element $x \notin G_0$. By compactness of G_0 there exists an open normal subgroup U of G such that $xU \cap G_0U = \emptyset$; then $(G/U)/(G_0U/U)$ is a finite abelian group of exponent p, and the image $\tilde{x}$ of x in $(G/U)/(G_0U/U)$ is nontrivial. Since $(G/U)/(G_0U/U)$ is a finite direct sum of the form $\bigoplus \mathbf{Z}/p\mathbf{Z}$, there is a maximal subgroup of $(G/U)/(G_0U/U)$ missing $\tilde{x}$. Hence there exists a maximal open subgroup of G missing x, and thus $x \notin \Phi(G)$. □

Corollary 2.8.8 *Let p be a prime number and $\psi : G_1 \longrightarrow G_2$ a continuous homomorphism of pro-p groups. Then*

(a) *$\psi(\Phi(G_1)) \leq \Phi(G_2)$. In particular, if $G_1 \leq G_2$, then $\Phi(G_1) \leq \Phi(G_2)$;*
(b) *If ψ is an epimorphism, then $\psi(\Phi(G_1)) = \Phi(G_2)$. In this case, ψ induces a continuous epimorphism $\bar{\psi} : G_1/\Phi(G_1) \longrightarrow G_2/\Phi(G_2)$.*

Proof. This follows immediately from Lemma 2.8.7(c). □

We remark that if $G_1 \leq G_2$ are profinite groups, then it is not necessarily true that $\Phi(G_1) \leq \Phi(G_2)$. For example, let G_2 a finite nonabelian simple group and G_1 a nonelementary abelian p-Sylow subgroup.

Proposition 2.8.9 *Let p be a prime number and let G be a pro-p group. Consider a family $\{H_i \mid i \in I\}$ of closed subgroups of G filtered from below. Let $H = \bigcap_{i\in I} H_i$. Then $\Phi(H) = \bigcap_{i\in I} \Phi(H_i)$.*

Proof. By Corollary 2.8.8 $\Phi(H) \leq \Phi(H_i)$ for each $i \in I$; hence $\Phi(H) \leq \bigcap_{i\in I} \Phi(H_i)$. To prove the opposite containment, let $x \in \bigcap_{i\in I} \Phi(H_i)$. Consider a maximal open normal subgroup U of H and denote by $\varphi : H \longrightarrow H/U$ the canonical epimorphism. We must show that $\varphi(x) = 1$. Choose $N \triangleleft_o G$ so that $N \cap H \leq U$. Then there exists some H_k with $H_k \leq NH$ (see Proposition 2.1.5). Denote by ψ the composition of natural maps

$$H_k \hookrightarrow NH \longrightarrow NH/N \cong H/N \cap H \longrightarrow H/U.$$

Clearly φ is the restriction of ψ to H. By Corollary 2.8.8, $\psi(x) = 1$ since $x \in \Phi(H_k)$ and $\Phi(H/U) = 1$; therefore, $\varphi(x) = 1$. □

For a pro-p group G there is a very useful way of characterizing when G is finitely generated in terms of its Frattini subgroup.

Proposition 2.8.10 *Let p be a prime number. A pro-p group G is finitely generated if and only if $\Phi(G)$ is an open subgroup of G.*

Proof. A maximal closed subgroup of a pro-p group G has index p (see Lemma 2.8.7). Therefore if G is finitely generated, it has only finitely many maximal closed subgroups (see Proposition 2.5.1). Hence their intersection has finite index, and so $\Phi(G)$ is open. Conversely, assume that $\Phi(G)$ is open. Then $G/\Phi(G)$ is a finite group; so there exists a finite subset X of G such that its image in $G/\Phi(G)$ generates this group, that is, $G = \overline{\langle X\rangle}\Phi(G)$. We deduce from Corollary 2.8.5 that $G = \overline{\langle X\rangle}$. □

In contrast with this result, remark that $\widehat{\mathbf{Z}}$ is procyclic, but its Frattini subgroup $\Phi(\widehat{\mathbf{Z}}) = \prod_p p\mathbf{Z}_p$ has infinite index. However, if the order of an abelian group G involves only a finite number of prime numbers, the analog to Proposition 2.8.10 still holds. More generally, one has the following result. Recall that a finite group G is *supersolvable* if it admits a finite series $G = C_0 \geq G_1 \geq \cdots \geq G_n = 1$ such that $G_i \triangleleft G$ and G_i/G_{i+1} is cyclic, for all i.

Proposition 2.8.11 *Let G be a prosupersolvable group whose order is divisible by only finitely many primes. Then G is finitely generated if and only if $\Phi(G)$ is open in G.*

Proof. If $\Phi(G)$ is open, then $G/\Phi(G)$ is a finite group. So $G = X\Phi(G)$ for some finite subset X of G. Hence $G = \overline{\langle X\rangle}$. Conversely, assume that G is finitely generated. It is known (cf. Hall [1959], Corollary 10.5.1) that the maximal subgroups of a finite supersolvable group are of prime index. It follows that the maximal open subgroups of the prosupersolvable group G have prime index as well. Since $\#G$ involves only finitely many primes, then the number of maximal open subgroups of G is finite. Hence their intersection $\Phi(G)$ is also open. □

Using this one can deduce the following proposition (cf. Oltikar and Ribes [1978] for a detailed proof).

Proposition 2.8.12 *Let G be a finitely generated prosupersolvable group. Then every p-Sylow subgroup of G is finitely generated.*

For a profinite group G define $\Phi^1(G) = \Phi(G)$ and inductively $\Phi^{n+1}(G) = \Phi(\Phi^n(G))$ for $n = 1, 2, \ldots$. The series

$$G \geq \Phi(G) \geq \Phi^2(G) \geq \cdots$$

is called the *Frattini series*. Clearly if $\Phi^n(G) \neq 1$, $[\Phi^n(G) : \Phi^{n+1}(G)] > 1$; hence if G is a finite group, its Frattini series leads to 1 in a finite number of steps, that is, $\Phi^n(G) = 1$ for some n.

Proposition 2.8.13 *Let p be a prime number and G a finitely generated pro-p group. Then the Frattini series of G constitutes a fundamental system of open neighborhoods of 1 in G.*

Proof. By Proposition 2.8.10 $\Phi(G)$ is open and hence finitely generated (see Proposition 2.5.5). We deduce inductively that each of the subgroups $\Phi^n(G)$ is open and finitely generated. To complete the proof we must show that if U is an open normal subgroup of G, then U contains $\Phi^n(G)$ for some n. Now, since G/U is a finite p-group, $\Phi^n(G/U) = 1$ for some n; finally observe that $\Phi^n(G/U) = \Phi^n(G)U/U$, as can be easily seen from Lemma 2.8.7 and induction on n. Thus $\Phi^n(G) \leq U$. □

Exercise 2.8.14 Let p be a prime number and G a pro-p group. Put

$$P_1(G) = G \quad \text{and} \quad P_{n+1}(G) = \overline{P_n(G)^p[G, P_n(G)]} \quad \text{for } n = 1, 2, \ldots.$$

Then

(a) For $K \triangleleft_c G$, $P_n(G/K) = P_n(G)K/K$, $(n = 1, 2, \ldots)$;
(b) $P_n(G)/P_{n+1}(G)$ is an elementary abelian p-group;
(c) $[P_n(G), P_m(G)] \leq P_{n+m}(G)$ for all natural numbers n, m;
(d) The series
$$G = P_1(G) \geq P_2(G) \geq \cdots \geq P_n(G) \geq \cdots$$
is a central series, that is, $P_n(G)/P_{n+1}(G)$ is in the center of $G/P_{n+1}(G)$ for all $n \geq 1$ (this series is called the *lower p-central series* of G);
(e) Assume that G is in addition finitely generated as a pro-p group. Then the subgroups $P_n(G)$ $(n = 1, 2, \ldots)$ form a fundamental system of open neighborhoods of 1 in G.

Lemma 2.8.15 *Let $\varphi : G \longrightarrow H$ be a continuous epimorphism of profinite groups. Then there exists a minimal closed subgroup K of G such that $\varphi(K) = H$. Moreover, if ψ denotes the restriction of φ to K, then* $\mathrm{Ker}(\psi) \leq \Phi(K)$.

Proof. We use Zorn's Lemma. Consider the collection $\mathcal{L}$ of all closed subgroups L of G with $\varphi(L) = H$; certainly $\mathcal{L} \neq \emptyset$. Order $\mathcal{L}$ by reversed inclusion. Consider a chain $\{L_i \mid i \in I\}$ in $\mathcal{L}$, that is, if $i, j \in I$ then either $L_i \leq L_j$ or $L_i \geq L_j$. We must show the existence of some $L \in \mathcal{L}$ such that $L \leq L_i$ for all $I \in I$. Define $L = \bigcap_{i\in I} L_i$. To see that $L \in \mathcal{L}$, we have to show that $\varphi(L) = H$, or equivalently, if $h \in H$ we need to prove that $\varphi^{-1}(h) \cap L \neq \emptyset$. Now, by assumption $\varphi^{-1}(h) \cap (\bigcap_{j\in J} L_j) \neq \emptyset$, for any finite subset J of I. Then, by the finite intersection property of compact spaces, we have $\varphi^{-1}(h) \cap L = \bigcap_{J\subseteq_f I}(\varphi^{-1}(h) \cap (\bigcap_{j\in J} L_j)) \neq \emptyset$, as desired. Therefore the poset $\mathcal{L}$ is inductive. The existence of K follows by Zorn's Lemma.

Consider now a maximal closed subgroup M of K. If $\mathrm{Ker}(\psi) \not\leq M$, then $M\mathrm{Ker}(\psi) = K$ and so $\varphi(M) = H$, contradicting the minimality of K. Thus $\mathrm{Ker}(\psi) \leq M$ for all maximal closed subgroups M of K, that is, $\mathrm{Ker}(\psi) \leq \Phi(K)$. □

A continuous epimorphism $\psi : K \longrightarrow H$ of profinite groups satisfying the conclusion of the lemma above (i.e., such that $\mathrm{Ker}(\psi) \leq \Phi(K)$) is called a *Frattini cover* of H.

Proposition 2.8.16 *Let p be a prime number and $A = \prod_I \mathbf{Z}/p\mathbf{Z}$ a direct product of copies of $\mathbf{Z}/p\mathbf{Z}$. Then every closed subgroup B of A has a direct complement C, that is, C is a closed subgroup of A such that $A = B \times C$.*

Proof. Consider the canonical epimorphism $\varphi : A \longrightarrow A/B$. By Lemma 2.8.15, there exists a closed subgroup C of A such that $\varphi(C) = A/B$ (that is, $A = BC$) and $B \cap C \leq \Phi(C)$. Since $pC = 0$, $\Phi(C) = 0$. Therefore, $B \cap C = 0$. Thus $A = B \times C$. □

2.9 Pontryagin Duality for Profinite Groups

Let X, Y be topological spaces. We begin with a definition for the compact-open topology on the space of all continuous functions $C(X, Y)$ from X to Y. For each compact subset K of X and each open subset U of Y, set

$$B(K, U) = \{f \in C(X, Y) \mid f(K) \subseteq U\}.$$

Then the collection of all subsets of the form $B(K, U)$ form a subbase for a topology on $C(X, Y)$; this topology is called the *compact-open topology* on $C(X, Y)$. If L is a subset of $C(X, Y)$, this topology induces on L a topology which is called the compact-open topology on L. (For general properties of the compact-open topology see, e.g., Bourbaki [1989], Section X.3.4].)

Denote by $\mathbf{T}$ the quotient group $\mathbf{T} = \mathbf{R}/\mathbf{Z}$ of the additive group of real numbers. Clearly $\mathbf{T}$ is isomorphic to the *circle group*, $\{e^{2\pi ix} \mid x \in \mathbf{R}\}$ consisting of all complex numbers of modulus 1. The *dual group* G^* of a locally compact abelian topological group G is defined to be the group

$$G^* = \mathrm{Hom}(G, \mathbf{T})$$

of all continuous homomorphisms from G to $\mathbf{T}$, endowed with the compact-open topology. It turns out that this topology makes G^* into a locally compact topological group. Denote by G^{**} the double dual of G, that is,

$$G^{**} = \mathrm{Hom}(G^*, \mathbf{T}) = \mathrm{Hom}(\mathrm{Hom}(G, \mathbf{T}), \mathbf{T}).$$

Given a group G, define a mapping

$$\alpha_G : G \longrightarrow G^{**}$$

by $\alpha_G(g) = g'$, where $g' : G^* \longrightarrow \mathbf{T}$ is the map given by $g'(f) = f(g)$ ($f \in G^*$). It is easy to check that α_G is a "natural" homomorphism, that is, it is a homomorphism, and whenever $\varphi : G \longrightarrow H$ is a group homomorphism and $\varphi^{**} : G^{**} \longrightarrow H^{**}$ the corresponding homomorphism of double duals, then the diagram

$$\begin{array}{ccc} G & \xrightarrow{\alpha_G} & G^{**} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi^{**}} \\ H & \xrightarrow[\alpha_H]{} & H^{**} \end{array}$$

commutes (in the language of categories, this says that α is a morphism from the identity functor on the category of groups to the double dual functor $\mathrm{Hom}(\mathrm{Hom}(-, \mathbf{T}), \mathbf{T})$).

The celebrated Pontryagin-van Kampen duality theorem establishes that if G is a locally compact abelian group, then α_G is an isomorphism of topological groups. A complete proof of this theorem requires considerable machinery and it is quite long. Proofs can be found for example in Hofmann and Morris [2006] Hewitt and Ross [1963], Morris [1977], Dikranjan, Prodanov and Stoyanov [1990].

The purpose of this section is to give a simple proof of Pontryagin-van Kampen's theorem in the especial case when G is profinite abelian or discrete torsion abelian. In order to do this we need first some lemmas.

Proposition 2.9.1

(a) *Every proper closed subgroup of* $\mathbf{T}$ *is finite.*
(b) *If G is compact, then G^* is discrete; and if G is discrete, then G^* is compact.*

Proof. Let $\varphi : \mathbf{R} \longrightarrow \mathbf{T} = \mathbf{R}/\mathbf{Z}$ denote the canonical epimorphism.

(a) It is well-known (and easy to prove) that every proper nondiscrete subgroup of the group $\mathbf{R}$ of real numbers is dense. Let A be a proper closed subgroup of $\mathbf{T}$. Then $\varphi^{-1}(A)$ is a proper closed subgroup of $\mathbf{R}$. Note that $\varphi^{-1}(A)$ is not dense in $\mathbf{R}$, for otherwise A would not be proper. Hence $\varphi^{-1}(A)$ is a discrete subgroup. Since φ is an open map, it follows that A is discrete. On the other hand, A is compact and thus finite.

(b) Assume that G is compact. Consider the open subset

$$U = \varphi(-1/3, 1/3)$$

of $\mathbf{T} = \mathbf{R}/\mathbf{Z}$. It is easy to see that the only subgroup of $\mathbf{T}$ contained in U is the trivial group $\{0\}$. Hence the subbasic open set $B(G, U)$ of G^* consists only of the zero map $\{0\}$. Thus G^* is discrete.

Assume now that G is discrete. Then the compact subsets of G are precisely the finite subsets. Hence the compact-open topology on G^* coincides with the topology induced on G^* from the direct product $\prod_G \mathbf{T} = \mathbf{T}^G$ with the usual product topology. We claim that G^* is a closed subset of $\prod_G \mathbf{T}$. Indeed, suppose that $f \in (\prod_G \mathbf{T}) - G^*$; then $f : G \longrightarrow \mathbf{T}$ is not a homomorphism. Therefore there exists $x, x' \in G$ with $f(xx') \neq f(x) + f(x')$. Choose disjoint open subsets U and V of $\mathbf{T}$ such that $f(xx') \in U$ and $f(x) + f(x') \in V$. Next choose neighborhoods W and W' of $f(x)$ and $f(x')$ respectively, such that $\alpha + \alpha' \in V$ whenever $\alpha \in W$ and $\alpha' \in W'$. Consider the open set H of $\mathbf{T}^G$ consisting of all maps $h : G \longrightarrow \mathbf{T}$ such that $h(xx') \in U$, $h(x) \in W$ and $h(x') \in W'$. Then H is a neighborhood of f in $\mathbf{T}^G$ such that $H \cap G^* = \emptyset$. This proves the claim. Then the compactness of $\mathbf{T}^G$ implies that G^* is compact. □

Lemma 2.9.2 *Let G be a profinite group and $f : G \longrightarrow \mathbf{T}$ a continuous homomorphism into the circle group $\mathbf{T} = \mathbf{R}/\mathbf{Z}$. Then*

(a) *$f(G)$ is a finite subgroup of $\mathbf{T}$; and*
(b) *f factors through the inclusion $\mathbf{Q}/\mathbf{Z} \hookrightarrow \mathbf{T}$, that is, $f(G) < \mathbf{Q}/\mathbf{Z}$.*

Proof. Since $\mathbf{T}$ is connected and $f(G)$ totally disconnected, then $\mathbf{T} \neq f(G)$. Hence $f(G)$ is finite (see Proposition 2.9.1(a)). Further, observe that the only torsion elements of $\mathbf{T}$ are those in $\mathbf{Q}/\mathbf{Z}$; so $f(G) < \mathbf{Q}/\mathbf{Z}$. □

Lemma 2.9.3

(a) *Let $\{G_i, \varphi_{ij}, I\}$ be a surjective inverse system of profinite groups over a directed poset I and let $G = \varprojlim_{i \in I} G_i$ be its inverse limit. Then there exists an isomorphism*

$$G^* = \mathrm{Hom}\Big(\varprojlim_{i \in I} G_i, \mathbf{T}\Big) \cong \varinjlim_{i \in I} \mathrm{Hom}(G_i, \mathbf{T}) = \varinjlim_{i \in I} G_i^*.$$

(b) *Let $\{A_i, \varphi_{ij}, I\}$ be a direct system of discrete torsion abelian groups over a directed poset I and let $A = \varinjlim_{i \in I} A_i$ be its direct limit. Assume that the canonical homomorphisms $\varphi_i : A_i \longrightarrow A$ are inclusion maps. Then there exists an isomorphism of profinite groups*

$$A^* = \mathrm{Hom}\Big(\varinjlim_{i \in I} A_i, \mathbf{T}\Big) \cong \varprojlim_{i \in I} \mathrm{Hom}(A_i, \mathbf{T}) = \varprojlim_{i \in I} A_i^*.$$

Proof. (a) Let $\varphi_i : G \longrightarrow G_i$ denote the projection of G onto G_i ($i \in I$). Let $f : G \longrightarrow \mathbf{T}$ be a continuous homomorphism; then $f(G)$ is a finite group by Lemma 2.9.2. Hence f factors through φ_j for some $j \in I$ (see Lemma 1.1.16), that is, there exists a homomorphism $f_j : G_j \longrightarrow \mathbf{T}$ such that $f = f_j\varphi_j$. Define

$$\Phi : G^* \longrightarrow \varinjlim_{i\in I} G_i^*$$

by $\Phi(f) = \tilde{f}_j$, where $\tilde{f}_j$ is the element of $\varinjlim_{i\in I} G_i^*$ represented by f_j. This is well-defined, for if f factors also through G_k, say $f = f_k\varphi_k$, one easily checks that $\tilde{f}_j = \tilde{f}_k$. Plainly Φ is an onto homomorphism. It is also a monomorphism, for if $\Phi(f) = \tilde{f}_j = 0$, then $f = f_r\varphi_r = 0$ for some $r \geq j$ (see Proposition 1.2.4).

(b) Denote by $\varphi_i : A_i \longrightarrow A$ the canonical homomorphism. Let

$$f : A = \varinjlim_{i\in I} A_i \longrightarrow \mathbf{T}$$

be a homomorphism. Denote by f_j the composition

$$A_j \xrightarrow{\varphi_j} A \xrightarrow{f} \mathbf{T}$$

($j \in I$). Then $(f_j) \in \varprojlim_{i\in I} \mathrm{Hom}(A_i, \mathbf{T})$. The map

$$\Psi : A^* \longrightarrow \varprojlim_{i\in I} A_i^*$$

given by $f \mapsto (f_j)$ is obviously an isomorphism of abstract groups. To see that Ψ is a topological isomorphism, it suffices to show that it is a continuous map, because the groups A^* and $\varprojlim_{i\in I} A_i^*$ are compact. Denote by

$$\rho_j : \varprojlim_{i\in I} A_i^* \longrightarrow A_j^*$$

the canonical projection ($j \in I$). Then Ψ is continuous if and only if $\rho_j\Psi$ is continuous for each $j \in I$. Consider a subbasic open set $B(K, U)$ of A_j^*, where K is a compact subset of A_j (hence finite) and where U is an open subset of $\mathbf{T}$. We must show that $(\rho_j\Psi)^{-1}(B(K, U))$ is open in A^*. Now, $\rho_j^{-1}(B(K, U))$ consists of all $(f_i) \in \varprojlim_{i\in I} A_i^*$ such that $f_j \in B(K, U)$. Identify K with its image in $A_j (\leq A)$. Then $(\rho_j\Psi)^{-1}(B(K, U))$ consists of all continuous homomorphisms $f : A \longrightarrow \mathbf{T}$ such that $f(K) \subseteq U$, that is, $(\rho_j\Psi)^{-1}(B(K, U))$ is a subbasic open set of A^*. □

To prove the following lemma one can use a slight variation of the above arguments. We leave the details to the reader.

Lemma 2.9.4

(a) *Let* $\{G_i \mid i \in I\}$ *be a collection of profinite groups. Then*

$$\left(\prod_{i\in I} G_i\right)^* \cong \bigoplus_{i\in I} G_i^*.$$

(b) *Let* $\{A_i \mid i \in I\}$ *be a collection of discrete torsion groups. Then*

$$\left(\bigoplus_{i\in I} A_i\right)^* \cong \prod_{i\in I} A_i^*.$$

Example 2.9.5

(1) If G is a finite abelian group, then $G^* \cong G$. To see this we may assume by Lemma 2.9.4 that G is cyclic. Say G is generated by x and the order of x is t. Let R_t be the unique subgroup of $\mathbf{T}$ consisting of the t-th roots of unity. Then $R_t \cong G$ and $\mathrm{Hom}(G, \mathbf{T}) = \mathrm{Hom}(G, R_t) \cong G$.
(2) $\mathbf{Z}_p^* \cong C_{p^\infty}$ and $C_{p^\infty}^* \cong \mathbf{Z}_p$. Indeed, these two statements follow from the example above and Lemma 2.9.3.
(3) $\widehat{\mathbf{Z}}^* \cong \mathbf{Q}/\mathbf{Z}$ and $(\mathbf{Q}/\mathbf{Z})^* \cong \widehat{\mathbf{Z}}$. To see this note that $\widehat{\mathbf{Z}} \cong \prod_p \mathbf{Z}_p$ and $\mathbf{Q}/\mathbf{Z} \cong \bigoplus_p C_{p^\infty}$, and apply Lemma 2.9.4.

Theorem 2.9.6 (Pontryagin Duality for Profinite Groups)

(a) *If* G *is either a profinite abelian group or a discrete abelian torsion group, then*

$$G^* = \mathrm{Hom}(G, \mathbf{T}) \cong \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z}).$$

(b) *The dual of a profinite abelian group is a discrete abelian torsion group, and the dual of a discrete abelian torsion group is a profinite abelian group.*
(c) *Let* G *be either a profinite abelian group or a discrete abelian torsion group. Then the homomorphism*

$$\alpha_G : G \longrightarrow G^{**}$$

is an isomorphism.

Proof. Part (a) is essentially the content of Lemma 2.9.2. Part (b) follows from Lemma 2.9.3 and Proposition 2.9.1. To prove part (c), note first that the result is obvious for finite cyclic groups. If G_1 and G_2 are groups, one easily checks that $\alpha_{G_1 \times G_2} = \alpha_{G_1} \times \alpha_{G_2}$. Since a finite abelian group is a direct product of cyclic groups, the result is valid for finite abelian groups.

Consider now a profinite abelian group G and express it as

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

where $\{G_i, \varphi_{ij}, I\}$ is a projective system of finite abelian groups. For each $i \in I$ we have a commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\alpha_G} & G^{**} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi^{**}} \\ G_i & \xrightarrow[\alpha_{G_i}]{} & G_i^{**} \end{array}$$

Using Lemma 2.9.3, one deduces that

$$\alpha_G = \varprojlim_{i \in I} \alpha_{G_i}.$$

Since each α_{G_i} is an isomorphism, so is α_G.

If, on the other hand, G is a discrete torsion abelian group, then G is the union of its finite subgroups, that is,

$$G = \varinjlim_{i \in I} G_i,$$

where each G_i is a finite abelian subgroup of G. Then

$$G^* = \mathrm{Hom}(G, \mathbf{T}) \cong \varprojlim_{i \in I} \mathrm{Hom}(G_i, \mathbf{T}).$$

So, using again Lemma 2.9.3,

$$G^{**} = \varinjlim_{i \in I} G_i^{**}$$

and $\alpha_G = \varinjlim_{i \in I} \alpha_{G_i}$; thus α_G is an isomorphism since each α_{G_i} is an isomorphism. □

Next we give some applications of this theorem that will be needed later.

Lemma 2.9.7 *Let G be a discrete torsion abelian group (respectively, profinite abelian group), H a subgroup (respectively, a closed subgroup) of G, and $g \in G - H$. Then there exists a homomorphism (respectively, a continuous homomorphism) $f : G \longrightarrow \mathbf{Q}/\mathbf{Z}$ such that $f(H) = 0$ and $f(g) \neq 0$.*

Proof. Replacing G by G/H if necessary, we may assume that $H = 0$, and we must show the existence of a (continuous) homomorphism f with $f(g) \neq 0$. If G is a discrete torsion abelian group, g has finite order; so there is a monomorphism $\langle g \rangle \hookrightarrow \mathbf{Q}/\mathbf{Z}$. Since $\mathbf{Q}/\mathbf{Z}$ is an injective abelian group (cf. Fuchs [1970], page 99), this monomorphism can be extended to a homomorphism $G \longrightarrow \mathbf{Q}/\mathbf{Z}$. If G is an abelian profinite group, consider a finite quotient G_i of G such that the image g_i of g in G_i is not trivial; then it suffices to construct a homomorphism $f_i : G_i \longrightarrow \mathbf{Q}/\mathbf{Z}$ with $f_i(g_i) \neq 0$. This follows again from the injectivity of $\mathbf{Q}/\mathbf{Z}$. □

If G is a discrete torsion (respectively, profinite) abelian group and H is a subgroup (respectively, closed subgroup) of G, denote by $\mathrm{Ann}_{G^*}(H)$ the *annihilator* of H in G^*, that is,

$$\mathrm{Ann}_{G^*}(H) = \{f \in G^* \mid f(h) = 0 \ \forall h \in H\}.$$

As an immediate consequence of the lemma above we have

Corollary 2.9.8 *Let G be a discrete torsion (respectively, profinite) abelian group and H is a subgroup (respectively, a closed subgroup) of G. Then*

$$H = \bigcap_{f \in \mathrm{Ann}_{G^*}(H)} \mathrm{Ker}(f).$$

Proposition 2.9.9 *Let G be a discrete torsion (respectively, profinite) abelian group and H is a subgroup (respectively, closed subgroup) of G. Then α_G sends H to $\mathrm{Ann}_{G^{**}}(\mathrm{Ann}_{G^*}(H))$ isomorphically. Equivalently, if we identify G with G^{**} via the topological isomorphism α_G, then*

$$\{g \in G \mid f(g) = 0 \ \forall f \in \mathrm{Ann}_{G^*}(H)\} = H$$

Proof. For $g \in G$ put $g' = \alpha_G(g)$. Then

$$\begin{aligned}\mathrm{Ann}_{G^{**}}(\mathrm{Ann}_{G^*}(H)) &= \{g' \in G^{**} \mid g'(f) = 0 \ \forall f \in \mathrm{Ann}_{G^*}(H)\}\\ &= \{g' \in G^{**} \mid f(g) = 0 \ \forall f \in \mathrm{Ann}_{G^*}(H)\}\\ &= \{h' \in G^{**} \mid h \in H\} = \alpha_G(H),\end{aligned}$$

where the penultimate equality follows from Corollary 2.9.8. □

Proposition 2.9.10 *Let G be a discrete torsion (respectively, profinite) abelian group and let H_1 and H_2 be subgroups (respectively, closed subgroups) of G. Then*

(a) $\mathrm{Ann}_{G^*}(H_1H_2) = \mathrm{Ann}_{G^*}(H_1) \cap \mathrm{Ann}_{G^*}(H_2)$;
(b) $\mathrm{Ann}_{G^*}(H_1 \cap H_2) = \mathrm{Ann}_{G^*}(H_1)\mathrm{Ann}_{G^*}(H_2)$.

Proof. Statement (a) is plain. According to Corollary 2.9.8, part (b) will follow if we can prove that

$$\mathrm{Ann}_{G^{**}}(\mathrm{Ann}_{G^*}(H_1 \cap H_2)) = \mathrm{Ann}_{G^{**}}(\mathrm{Ann}_{G^*}(H_1)\mathrm{Ann}_{G^*}(H_2)).$$

Using part (a), Proposition 2.9.9 and the fact that α_G is an isomorphism (the duality theorem), we have

$$\begin{aligned}&\mathrm{Ann}_{G^{**}}(\mathrm{Ann}_{G^*}(H_1)\mathrm{Ann}_{G^*}(H_2))\\ &\quad = \mathrm{Ann}_{G^{**}}(\mathrm{Ann}_{G^*}(H_1)) \cap \mathrm{Ann}_{G^{**}}(\mathrm{Ann}_{G^*}(H_2))\\ &\quad = \alpha_G(H_1) \cap \alpha_G(H_2) = \alpha_G(H_1 \cap H_2) = \mathrm{Ann}_{G^{**}}(\mathrm{Ann}_{G^*}(H_1 \cap H_2)),\end{aligned}$$

as needed. □

Let G be a group and n a natural number. Put

$$G^n = \{x^n \mid x \in G\}$$

and

$$G[n] = \{x \in G \mid x^n = 1\}.$$

Observe that if G is abelian, then both G^n and $G[n]$ are subgroups of G. If G is a profinite abelian group, then both G^n and $G[n]$ are closed subgroups of G.

Lemma 2.9.11 *Let G be an abelian group which is either profinite or discrete. Fix a natural number n. Then*

(a) $\mathrm{Ann}_{G^*}(G^n) = (G^*)[n]$;
(b) $\mathrm{Ann}_{G^*}(G[n]) = (G^*)^n$.

Proof. (a) $\mathrm{Ann}_{G^*}(G^n) = \{f \in G^* \mid f(x^n) = 0, \forall x \in G\} = \{f \in G^* \mid (nf)(x) = 0, \forall x \in G\} = \{f \in G^* \mid nf = 0\} = (G^*)[n]$

(b) By Proposition 2.9.9 and part (a), we have (after identifying G and G^{**})

$$(G^*)^n = \mathrm{Ann}_{G^*}(\mathrm{Ann}_{G^{**}}((G^*)^n)) = \mathrm{Ann}_{G^*}(G^{**}[n]) = \mathrm{Ann}_{G^*}(G[n]).$$ □

Recall that an abelian group G is *divisible* if for every natural number n and for every element $x \in G$, there exists some element $y \in G$ such that $y^n = x$.

Theorem 2.9.12 *Let G be an abelian group which is either discrete or profinite. Then G is divisible if and only if G^* is torsion-free.*

Proof. Assume that G is divisible. Then $G = G^n$ for every natural number n. By Lemma 2.9.11,

$$0 = \mathrm{Ann}_{G^*}(G) = \mathrm{Ann}_{G^*}(G^n) = (G^*)[n]$$

for every natural number n. Therefore G^* is torsion-free.

To show the converse it suffices to prove, by Theorem 2.9.6, that if G is torsion-free, then G^* is divisible. Assume that G is torsion-free. Then $G[n] = 1$ for every natural number $n \geq 2$. Hence $\mathrm{Ann}_{G^*}(G[n]) = G^*$ for all $n \geq 2$. Therefore, by Lemma 2.9.11,

$$(G^*)^n = G^*$$

for all $n \geq 0$. Thus G^* is divisible. □

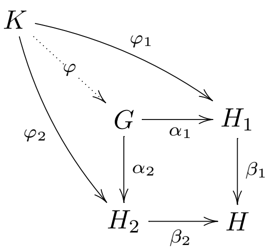
2.10 Pullbacks and Pushouts

In this section we establish the concepts of pullback and pushout diagrams. We do this only for profinite groups and we leave to the reader the development of the analogous constructions for other categories, like modules, graphs, etc. For a more general treatment of these concepts in a category, see for example Mac Lane [1971].

A commutative square diagram

$$\begin{array}{ccc} G & \xrightarrow{\alpha_1} & H_1 \\ {\scriptstyle \alpha_2}\downarrow & & \downarrow{\scriptstyle \beta_1} \\ H_2 & \xrightarrow[\beta_2]{} & H \end{array} \tag{4}$$

of profinite groups and continuous homomorphisms is called a *pullback diagram* or a *pullback of* β_1 *and* β_2 if the following universal property is satisfied:



whenever K is a profinite group and $\varphi_i : K \longrightarrow H_i$ $(i = 1, 2)$ are continuous homomorphisms such that $\beta_1\varphi_1 = \beta_2\varphi_2$, then there exists a unique continuous homomorphism $\varphi : K \longrightarrow G$ such that $\alpha_1\varphi = \varphi_1$ and $\alpha_2\varphi = \varphi_2$.

We say that φ is the canonical homomorphism determined by φ_1 and φ_2. Given two continuous homomorphisms of profinite groups $\beta_i : H_i \longrightarrow H$, there exists a (essentially unique) pullback of β_1 and β_2. Indeed, define

$$P = \{(h_1, h_2) \in H_1 \times H_2 \mid \beta_1(h_1) = \beta_2(h_2)\};$$

and let $\gamma_i : P \longrightarrow H_i$ be given by $\gamma_i(h_1, h_2) = h_i$ $(i = 1, 2)$. Then

$$\begin{array}{ccc} P & \xrightarrow{\gamma_1} & H_1 \\ {\scriptstyle \gamma_2}\downarrow & & \downarrow{\scriptstyle \beta_1} \\ H_2 & \xrightarrow[\beta_2]{} & H \end{array}$$

is a pullback diagram, as one easily checks. It is unique in the sense that if (4) is also a pullback of β_1 and β_2, then there exists a continuous homomorphism

$$\alpha : G \longrightarrow P$$

such that $\gamma_i\alpha = \alpha_i$ $(i = 1, 2)$; namely α is given $\alpha(g) = (\alpha_1(g), \alpha_2(g))$; moreover, one verifies with no difficulty that α is an isomorphism.

Exercise 2.10.1 Let U, V be closed normal subgroups of a profinite group G. Then the commutative square of natural epimorphisms

$$\begin{array}{ccc} G/U\cap V & \longrightarrow & G/U \\ \downarrow & & \downarrow \\ G/V & \longrightarrow & G/UV \end{array}$$

is a pullback diagram.

Lemma 2.10.2 *Assume that* (4) *is a pullback diagram of profinite groups. Let A be a profinite group and let $\varphi_i : A \longrightarrow H_i$ $(i = 1, 2)$ be continuous epimorphisms such that $\beta_1\varphi_1 = \beta_2\varphi_2$ and* $\mathrm{Ker}(\beta_1\varphi_1) = \mathrm{Ker}(\varphi_1)\mathrm{Ker}(\varphi_2)$. *Then the canonical homomorphism $\varphi : A \longrightarrow G$ determined by φ_1 and φ_2 is an epimorphism.*

Proof. As pointed out above, G can be identified with

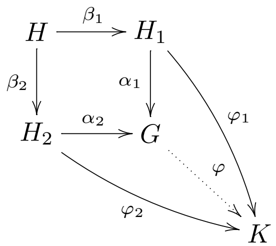
$$\{(h_1, h_2) \in H_1 \times H_2 \mid \beta_1(h_1) = \beta_2(h_2)\}$$

and α_1 and α_2 with the natural projections. Note that in this case, $\varphi(a) = (\varphi_1(a), \varphi_2(a))$, for all $a \in A$. Since $\alpha_1\varphi = \varphi_1$ is onto, to prove that φ is an epimorphism, it suffices to show that $\mathrm{Ker}(\alpha_1) \leq \varphi(A)$; in fact we shall show that $\mathrm{Ker}(\beta_1\alpha_1) \leq \varphi(A)$. Let $(h_1, h_2) \in \mathrm{Ker}(\beta_1\alpha_1)$. We infer that $h_i \in \mathrm{Ker}(\beta_i)$ $(i = 1, 2)$. Let $a \in A$ with $\varphi_1(a) = h_1$. Then $a \in \mathrm{Ker}(\beta_1\varphi_1) = \mathrm{Ker}(\varphi_1)\mathrm{Ker}(\varphi_2)$. Hence $a = k_1k_2$, where $k_i \in \mathrm{Ker}(\varphi_i)$ $(i = 1, 2)$. Therefore, $h_1 = \varphi_1(k_2)$. Similarly, $h_2 = \varphi_2(l_1)$ for some $l_1 \in \mathrm{Ker}(\varphi_1)$. Thus, $\varphi(l_1k_2) = (h_1, h_2)$. Thus φ is onto. □

The dual concept of pullback is that of pushout. Specifically, a commutative square diagram

$$\begin{array}{ccc} H & \xrightarrow{\beta_1} & H_1 \\ {\scriptstyle\beta_2}\downarrow & & \downarrow{\scriptstyle\alpha_1} \\ H_2 & \xrightarrow[\alpha_2]{} & G \end{array}$$

of profinite groups and continuous homomorphisms is called a *pushout diagram* or a *pushout of* β_1 *and* β_2 if the following universal property is satisfied:



whenever K is a profinite group and $\varphi_i : H_i \longrightarrow K$ $(i = 1, 2)$ are continuous homomorphisms such that $\varphi_1\beta_1 = \varphi_2\beta_2$, then there exists a unique continuous homomorphism $\varphi : G \longrightarrow K$ such that $\varphi\alpha_1 = \varphi_1$ and $\varphi\alpha_2 = \varphi_2$.

The existence of pushout diagrams of profinite groups will be established in Chapter 9.

2.11 Profinite Groups as Galois Groups

In this section we show that profinite groups are precisely those groups that are Galois groups of (finite or infinite) Galois extensions of fields, with an appropriate topology. Historically, this is the original motivation for the study of profinite groups and Galois theory remains the main area of applications of results in profinite groups.

Let K/F be an algebraic, normal and separable extension of fields, that is, a Galois extension. Consider the collection $\mathcal{K} = \{K_i \mid i \in I\}$ of all intermediate subfields $F \subseteq K_i \subseteq K$ such that each K_i/F is a finite Galois extension. Then

$$K = \bigcup_{i \in I} K_i.$$

Let $G = G_{K/F}$ and $U_i = G_{K/K_i}$ denote the Galois groups of K/F and K/K_i $(i \in I)$, respectively. Using elementary results in Galois theory, one sees that

(1) $U_i \lhd G$, and $G/U_i \cong G_{K_i/F}$ is finite for every $i \in I$;
(2) If $i, j \in I$, then there exists some $k \in I$ such that $U_k \leq U_i \cap U_j$; and
(3) $\bigcap_{i \in I} U_i = \{1\}$.

Then there is a unique topology on G, compatible with the group structure of G, for which the collection $\{U_i \mid i \in I\}$ is a fundamental system of neighborhoods of the identity element 1 of G (cf. Bourbaki [1989], Ch. III, Proposition 1). This topology is called the *Krull topology* of the Galois group $G = G_{K/F}$. Note that if the Galois extension K/F is finite, then the Krull topology on $G = G_{K/F}$ is the discrete topology.

Theorem 2.11.1 *The Galois group $G = G_{K/F}$, endowed with the Krull topology, is a profinite group. Moreover,*

$$G_{K/F} = \varprojlim_{i \in I} G_{K_i/F}.$$

Proof. For each $i \in I$, consider the finite Galois group $G_i = G_{K_i/F}$. Observe that, with the above notation, $G_i \cong G/U_i$. Define a partial order relation $\preceq$ on the set I as follows. Let $i, j \in I$; then

$i \preceq j$ if $K_i \subseteq K_j$, or equivalently if $U_i = G_{K/K_i} \geq U_j = G_{K/K_j}$. Plainly $(I, \preceq)$ is a poset. In fact it is a directed poset. Indeed, if $K_i, K_j \in \mathcal{K}$, then there exist polynomials $f_i(X), f_j(X) \in F[X]$ such that K_i and K_j are the splitting fields contained in K of $f_i(X)$ and $f_j(X)$ over F, respectively. Let L be the splitting field over F of the polynomial $f_i(X)f_j(X)$, with $L \subseteq K$. Then $L \in \mathcal{K}$. Say $L = K_t$ for some $t \in I$. Then by definition $t \succeq i, j$.

If $i \preceq j$, define

$$\varphi_{ji} : G_j = G_{K_j/F} \longrightarrow G_i = G_{K_i/F}$$

by restriction, that is, $\varphi_{ji}(\sigma) = \sigma_{|K_i}$, where $\sigma \in G_{K_j/F}$. Observe that φ_{ji} is well-defined, because $\sigma(K_i) = K_i$ since K_i/F is a normal extension. We obtain in this manner an inverse system $\{G_i, \varphi_{ij}, I\}$ of finite Galois groups. Consider the homomorphism

$$\Phi : G = G_{K/F} \longrightarrow \varprojlim_{i \in I} G_i \leq \prod_{i \in I} G_i$$

defined by

$$\Phi(\sigma) = (\sigma_{|K_i}).$$

We shall show that Φ is an isomorphism of topological groups. It is a monomorphism since $\mathrm{Ker}(\Phi) = \bigcap_{i \in I} G_{K_i/F} = 1$. The homomorphism Φ is continuous since the composition

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

is continuous for each $i \in I$. Also, Φ is an open mapping since

$$\Phi(G_{K/K_i}) = (\varprojlim G_i) \cap \left[\left(\prod_{K_j \not\subseteq K_i} G_j \right) \times \left(\prod_{K_j \subseteq K_i} \{1\}_j \right) \right].$$

Finally, Φ is an epimorphism. Indeed, if $(\sigma_i) \in \varprojlim G_i$, define $\sigma : K \longrightarrow K$ by $\sigma(k) = \sigma_i(k)$ for $k \in K_i$; then $\sigma \in G$ and $\Phi(\sigma) = (\sigma_i)$. Thus we have proved that $G \cong \varprojlim G_i$. The result now follows from the characterization of profinite groups obtained in Theorem 2.1.3. □

Example 2.11.2

(1) Let p be a prime number, $\mathbf{F}_p$ the field with p elements, and let $\overline{\mathbf{F}}_p$ be its algebraic closure. Then the Galois group of the extension $\overline{\mathbf{F}}_p/\mathbf{F}_p$ is $\widehat{\mathbf{Z}}$. Indeed, from the theory of finite fields, for each positive integer n, there exists a unique Galois extension $K_n/\mathbf{F}_p$ of degree $[K_n : \mathbf{F}_p] = n$ and $G_{K_n/\mathbf{F}_p} \cong \mathbf{Z}/n\mathbf{Z}$. Thus it follows from Theorem 2.11.1 that

$$G_{\overline{\mathbf{F}}_p/\mathbf{F}_p} = \varprojlim_n \mathbf{Z}/n\mathbf{Z} = \widehat{\mathbf{Z}}.$$

(2) Let p and q be prime numbers. For each positive integer n, there is a unique field L_n with $\mathbf{F}_p \subseteq L_n \subseteq \overline{\mathbf{F}}_p$, such that $[L_n : \mathbf{F}_p] = q^n$. Then $L = \bigcup_{n=1}^{\infty} L_n$ is a Galois extension of $\mathbf{F}_p$, and

$$G_{L/\mathbf{F}_p} = \varprojlim G_{L_n/\mathbf{F}_p} = \varprojlim \mathbf{Z}/q^n\mathbf{Z} = \mathbf{Z}_q.$$

The Krull topology on the Galois group $G = G_{K/F}$ was introduced by Krull [1928]. His aim was to provide a generalization, to infinite Galois extensions, of the Galois correspondence between intermediate fields of (a finite Galois extension) K/F and the subgroups of the group $G_{K/F}$.

Theorem 2.11.3 *Let K/F be a Galois extension of fields with Galois group $G = G_{K/F}$. Denote by $\mathcal{F}(K/F)$ the set of intermediate fields $F \subseteq L \subseteq K$. Endow G with the Krull topology and let $\mathcal{S}(G)$ denote the set of closed subgroups of G. Consider the map*

$$\Phi : \mathcal{F}(K/F) \longrightarrow \mathcal{S}(G)$$

defined by

$$\Phi(L) = \{\sigma \in G_{K/F} \mid \sigma_{|L} = \mathrm{id}_L\}.$$

Then Φ is a bijection that reverses inclusion, that is, if $L_1 \subseteq L_2$ are fields in $\mathcal{F}(K/F)$, then $\Phi(L_1) \geq \Phi(L_2)$. The inverse of Φ is the map

$$\Psi : \mathcal{S}(G) \longrightarrow \mathcal{F}(K/F)$$

given by

$$\Psi(H) = \{x \in K \mid \sigma(x) = x, \forall \sigma \in H\}.$$

Moreover, $L \in \mathcal{F}(K/F)$ is a normal extension of F if and only if $\Phi(L)$ is a normal subgroup of G, and if that is the case, $G_{L/F} \cong G/\Phi(L)$.

Proof. It is clear that $\Phi(L)$ reverses inclusion. Observe that $\Phi(L) = G_{K/L}$; furthermore, the Krull topology on $G_{K/L}$ is the topology induced from $G = G_{K/F}$, and since, according to Theorem 2.11.1, $G_{K/L}$ is compact, then it is closed in G; therefore $\Phi(L) \in \mathcal{S}(G)$. Next, we check that $\Psi\Phi(L) = L$ for all $L \in \mathcal{F}(K/F)$. Obviously $\Psi\Phi(L) = \Psi(G_{K/L}) \supseteq L$. Finally, if $y \in K$ and y is fixed by every automorphism $\sigma \in G_{K/L}$, then the minimal polynomial of y over L must be of degree 1; so $y \in L$.

Conversely, let us show that $\Phi\Psi(H) = H$ for every closed subgroup H of G. Put $L = \Psi(H)$. Plainly, $\Phi\Psi(H) = G_{K/L} \supseteq H$. To see that $G_{K/L} = H$, it will suffice to show that H is dense in $G_{K/L}$, since H is closed. Now, let N be an intermediate extension of K/L such that N/L is a finite Galois extension. Let $\tau \in G_{K/L}$; we need to show that $\tau G_{K/N} \cap H \neq \emptyset$. Remark that if $\sigma \in H$, then $\sigma(N) = N$, so $\{\sigma_{|N} \mid \sigma \in H\}$ is a group of automorphisms of N fixing the elements of L; hence, by the fundamental theorem of Galois theory for finite field extensions (cf. Bourbaki [1967], V,10,5, Theorem 3),

$$\{\sigma_{|N} \mid \sigma \in H\} = G_{N/L}.$$

Then there exists some $\sigma \in H$ such that $\tau_{|N} = \sigma_{|N}$; therefore, $\sigma \in \tau G_{K/N}$, as desired.

Assume now that $L \in \mathcal{F}(K/F)$ and L/F is a normal extension. Let $\sigma \in G_{K/L}, \tau \in G_{K/F}$. Evidently, $\tau^{-1}\sigma\tau \in G_{K/L}$ and so $\Phi(L) = G_{K/L} \triangleleft G_{K/F} = G$. Recall that every F-automorphism of L can be extended to an F-automorphism of K (cf. Bourbaki [1967], V,6,3, Proposition 7). On the other hand, if L/F is normal, then $\tau(L) = L$, for all $\tau \in G = G_{K/F}$. Therefore there is a natural epimorphism

$$G = G_{K/F} \longrightarrow G_{L/F}$$

given by restriction $\tau \mapsto \tau_{|L}$. The kernel of this epimorphism is $\Phi(L) = G_{K/L}$; thus $G_{L/F} \cong G/\Phi(L)$.

Conversely, if $\Phi(L) = G_{K/L} \triangleleft G_{K/F} = G$, it follows that $\tau(L) = L$ for each $\tau \in G = G_{K/F}$. This implies that L/F is a normal extension (cf. Bourbaki [1967], V,6,3, Proposition 6). □

Exercise 2.11.4 Let p be a prime number. Let $\mathbf{F}_p$ be the field with p elements, and $\overline{\mathbf{F}}_p$ its algebraic closure. Prove that the Galois group $G_{\overline{\mathbf{F}}_p/\mathbf{F}_p} \cong \widehat{\mathbf{Z}}$ is topologicaly generated by the Frobenius automorphism $\varphi : \overline{\mathbf{F}}_p \longrightarrow \overline{\mathbf{F}}_p$ given by $\varphi(x) = x^p$. Exhibit explicitly a nonclosed subgroup H of $G_{\overline{\mathbf{F}}_p/\mathbf{F}_p}$ whose fixed field is $\mathbf{F}_p$ (the fixed field of $G_{\overline{\mathbf{F}}_p/\mathbf{F}_p}$).

As we have seen in Theorem 2.11.1, every Galois group can be interpreted as a profinite group. In the next theorem we show that, conversely, every profinite group can be realized as a Galois group of an appropriate Galois extension of fields.

Theorem 2.11.5 *Let G be a profinite group. Then there exists a Galois extension of fields K/L such that $G = G_{K/L}$.*

Proof. Let F be any field. Denote by T the disjoint union of all the sets G/U, where U runs through the collection of all open normal subgroups of G. Think of the elements of T as indeterminates, and consider the field $K = F(T)$ of all rational functions on the indeterminates in T with coefficients in F. The group G operates on T in a natural manner: if $\gamma \in G$ and $\gamma' U \in G/U$, then $\gamma(\gamma' U) = \gamma\gamma' U$. This in turn induces an action of G on K as a group of F-automorphisms of K. Put $L = K^G$, the subfield of K consisting of the elements of K fixed by all the automorphisms $\gamma \in G$. We shall show that K/L is a Galois extension with Galois group G.

If $k \in K$, consider the subgroup

$$G_k = \{\gamma \in G \mid \gamma(k) = k\}$$

of G. If the indeterminates that appear in the rational expression of k are $\{t_i \in G/U_i \mid i = 1, \dots, n\}$, then

$$G_k \supseteq \bigcap_{i=1}^{n} U_i.$$

Therefore G_k is an open subgroup of G, and hence of finite index. From this we deduce that the orbit of k under the action of G is finite. Say that $\{k = k_1, k_2, \ldots, k_r\}$ is the orbit of k. Consider the polynomial

$$f(X) = \prod_{i=1}^{r} (X - k_i).$$

Since G transforms this polynomial into itself, its coefficients are in L, that is, $f(X) \in L[X]$. Hence k is algebraic over L. Moreover, since the roots of $f(X)$ are all different, k is separable over L. Finally, the extension $L(k_1, k_2, \ldots, k_r)/L$ is normal. Hence K is a union of normal extensions over L; thus K/L is a normal extension. Therefore K/L is a Galois extension. Let H be the Galois group of K/L; then G is a subgroup of H. To show that $G = H$, observe first that the inclusion mapping $G \hookrightarrow H$ is continuous, for assume that $U \triangleleft_o H$ and let K^U be the subfield of the elements fixed by U; then K^U/L is a finite Galois extension by Theorem 2.11.3; say, $K^U = L(k'_1, \ldots, k'_s)$ for some $k'_1, \ldots, k'_s \in K$. Then

$$G \cap U \supseteq \bigcap_{i=1}^{s} G_{k'_i}.$$

Therefore $G \cap U$ is open in G. This shows that G is a closed subgroup of H. Finally, since G and H fix the same elements of K, it follows from Theorem 2.11.3 that $G = H$. □

2.12 Notes, Comments and Further Reading

As pointed out in Section 2.11, interest about general profinite groups appeared first among algebraic number theorists. Krull [1928] defined a natural topology on the Galois group $G_{K/F}$ (usually called now the Krull topology) with the idea of making precise the generalization of the fundamental theorem of Galois theory in the case of extensions of infinite degree (see Theorem 2.11.3). With this topology the Galois group becomes a profinite group (see Theorem 2.11.1).

Profinite groups were first called 'groups of Galois type'; the first systematic presentation of these groups appeared in the influential book Cohomologie Galoisienne by Serre [1995] whose first edition is of 1964; this book has served as a source of information and inspiration to mathematicians, including the authors of the present book, since then. In this book Serre refers to these groups as 'profinite' and 'pro-p' groups to the exclusion of any other terminology. Serre's book contains a systematic use of properties of profinite and pro-p groups to field theory. It is a short volume, written in a very terse style, that contains a wealth of results and information. Books published later by Poitou [1967], Koch [1970], Ribes [1970], Shatz [1972], Fried and Jarden [2008] and most recently, Dixon, du Sautoy, Mann and Segal [1999], Klaas, Leedham-Green and Plesken [1997], Wilson [1998] concentrate on special aspects of the theory, and are generally more detailed. Serre's book is the best source for certain material, e.g., nonabelian cohomology and applications to field theory.

Some particular profinite groups have a much older history, also rooted in number theory. The group $\mathbf{Z}_p$ of p-adic integers was first defined by Hensel during his studies of algebraic numbers; see Hensel [1908]. Theorem 2.11.5 was first proved by Leptin [1955]; see also Waterhouse [1972]. The proof of this theorem that we present here is taken from Ribes [1977].

Proposition 2.2.2, Exercise 2.2.3, Corollary 2.3.6 and Proposition 2.4.4 appear in Douady [1960], where they are attributed to Tate. Many of the basic results about profinite groups, including cohomological ones, were first established by Tate, but he has not published much on the subject; see Lang [1966], Tate [1962]. See also Appelgate and Onishi [1977], Borovik, Pyber and Shalev [1996], Brauer [1969]. The notion of 'supernatural number' is due to Steinitz [1910], page 250; he uses instead the term 'G-number', but we have decided to stay with the terminology of 'supernatural' because it is well-entrenched by now in the literature and because it is very expressive.

Corollary 2.3.7 can be found in Bolker [1963]. Exercise 2.3.14 appears in Gilotti, Ribes and Serena [1999]; this paper contains results relating to fusion and transfer in the context of profinite groups. Exercise 2.3.17 appears in Lim [1973a]. For a study of localization in profinite groups see Herfort and Ribenboim [1984].

Proposition 2.5.4 was proved in Gaschütz [1956] for finite groups. The proof that we give here is attributed to Roquette in Fried and Jarden [2008]. Corollary 2.6.6 is due to Iwasawa [1953]. See Joly [1965], for a study of procyclic groups. The basic properties of the Frattini subgroup in the context of profinite groups are given in Gruenberg [1967]. Propositions 2.8.2(c) and 2.8.11 appear in Oltikar and Ribes [1978]. Proposition 2.8.9 was proved by Lubotzky [1982]. Lemma 2.8.15 and the concept of Frattini cover can be found in Cossey, Kegel and Kovács [1980]; for additional information on results and applications of Frattini covers, see Ershov [1980], Ershov and Fried [1980], Haran and Lubotzky [1983], Cherlin, van den Dries and Macintyre [1984], Ribes [1985]. For a result on direct products, see Goldstein and Guralnick [2006].

2.12.1 Analytic Pro-p Groups

Let G be a finitely generated profinite group. According to Proposition 2.5.5, every open subgroup U of G is also finitely generated. However the minimal number $d(U)$ of generators of U is usually unbounded (see Theorem 3.6.2(b) for the case of free profinite groups). More generally, if H is a closed subgroup of G, then one can usually say little about $d(H)$. Nevertheless, there is an important class of finitely generated profinite groups G for which

$$\max\{d(H) \mid H \leq_c G\} = r(G) < \infty.$$

(The number $r(G)$ thus defined is sometimes called the 'rank' of the group G; we refrain from this terminology to avoid confusion with the concept of rank of a free group which will be introduced in Chapter 3.)

A representative example of such groups is $G = \mathrm{GL}_n(\mathbf{Z}_p)$. This group contains an open pro-p subgroup K_1 of index $(p^n - 1)(p^{n-1} - 1)\cdots(p-1)$ (see Exercise 2.3.12). One can then prove the following result (see, e.g., Dixon, du Sautoy, Mann and Segal [1999], Theorem 5.2):

Theorem 2.12.1a $r(K_1) = n^2$. *Consequently,* $r(G) < \infty$.

Profinite groups satisfying conditions analogous to those mentioned above for $\mathrm{GL}_n(\mathbf{Z}_p)$ are called *p-adic analytic groups*. Explicitly, a profinite group G is p-adic analytic if it contains an open pro-p subgroup H such that $r(H) < \infty$. The reason for this terminology is the following theorem due to Lazard (see Lazard [1965], III, 3.4). Let $\mathbf{Q}_p$ be the field of p-adic numbers, that is, the field of quotients of $\mathbf{Z}_p$.

Theorem 2.12.1b *Let G be a Hausdorff topological group. Then G is p-adic analytic if and only if G is compact and admits a structure of a $\mathbf{Q}_p$-manifold in such a way that multiplication and inversion in G are analytic functions.*

Research in the theory of profinite p-adic analytic groups and related topics is presently very active. An excellent modern exposition can be found in Dixon, du Sautoy, Mann and Segal [1999]. See also Lazard [1965, 1954] (these two works contain a large amount of information on these and other topics rarely found elsewhere), Lubotzky and Mann [1989], Lubotzky and Segal [2003], Mann and Segal [1990], du Sautoy [1993], du Sautoy and Grunewald [2002], Fernández-Alcober, González-Sánchez and Jaikin-Zapirain [2008], Shalev [1992]. See also Detomi and Lucchini [2007].

2.12.2 Number of Generators of a Group and of Its Profinite Completion

Let G be a finitely generated residually finite abstract group and consider its profinite completion $\widehat{G}$. We denote by $d(G)$ the minimal cardinality of a set of generators of G as an abstract group; while $d(\widehat{G})$ denotes the minimal cardinality of a set of generators of $\widehat{G}$ as a profinite group. Obviously $d(\widehat{G}) \leq d(G)$. Put $f(G) = d(G) - d(\widehat{G})$. Then one has the following results.

Theorem 2.12.2a (Noskov [1983]) *For each natural number n, there exist a finitely generated abstract metabelian group G_n such that $f(G_n) \geq n$.*

On the other hand, for polycyclic groups G one has

Theorem 2.12.2b (Linnell and Warhurst [1981]) *If G is a polycyclic group, then $f(G) \leq 1$.*

3 Free Profinite Groups

3.1 Profinite Topologies

Let $\mathcal{N}$ be a nonempty collection of normal subgroups of finite index of a group G and assume that $\mathcal{N}$ is filtered from below, i.e., $\mathcal{N}$ satisfies the following condition:

$$\text{whenever } N_1, N_2 \in \mathcal{N}, \text{ there exists } N \in \mathcal{N} \text{ such that } N \leq N_1 \cap N_2.$$

Then one can make G into a topological group by considering $\mathcal{N}$ as a fundamental system of neighborhoods of the identity element 1 of G (cf. Bourbaki [1989]. Ch. 3, Proposition 1). We refer to the corresponding topology on G as a *profinite topology.* If every quotient G/N ($N \in \mathcal{N}$) belongs to a certain class $\mathcal{C}$, we say more specifically that the topology above is *a pro-$\mathcal{C}$ topology.*

Let $\mathcal{C}$ be a formation of finite groups, and let G be a group. Define

$$\mathcal{N}_{\mathcal{C}}(G) = \{N \triangleleft_f G \mid G/N \in \mathcal{C}\}. \tag{1}$$

Then $\mathcal{N}_{\mathcal{C}}(G)$ is nonempty and filtered from below. The corresponding profinite topology on G is called the *pro-$\mathcal{C}$ topology of G* or, if emphasis is needed, *the full pro-$\mathcal{C}$ topology of G*. Note that the pro-$\mathcal{C}$ topology of G is Hausdorff if and only if

$$\bigcap_{N \in \mathcal{N}_{\mathcal{C}}(G)} N = 1. \tag{2}$$

A group G is called *residually* $\mathcal{C}$ if it satisfies condition (2).

Remark 3.1.1 Assume that a profinite topology on G is determined by a collection $\mathcal{N}$ of normal subgroups of finite index filtered from below. Consider the set $\mathcal{C}$ of all groups G/M, where M ranges over all open normal subgroups of G. Then $\mathcal{C}$ is a formation of finite groups, and the given topology on G is a pro-$\mathcal{C}$ topology of G, although not necessarily the full pro-$\mathcal{C}$ topology of G. Indeed, consider a finite group T of order $n > 1$, and let G be the direct product of infinitely many copies of T. Let $\mathcal{N}$ be the collection of all the open normal subgroups of the profinite group G, and let $\mathcal{C}$ be as indicated above. As we shall show in Example 4.2.12, the pro-$\mathcal{C}$ topology of G is richer than its natural profinite topology.

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4_3,

If $\mathcal{C}$ is the class of all finite groups (respectively, all finite p-groups, or all finite solvable groups, etc.), then, instead of residually $\mathcal{C}$, we say that G is a *residually finite group* (respectively, a *residually finite p-group* or a *residually finite solvable group*, etc.). The corresponding topology on G is called *the* (*full*) *profinite topology* on G (respectively, *the* (*full*) *pro-p topology, the* (*full*) *prosolvable topology* etc. on G). We remark that, for example, the full pronilpotent topology on a group G is a prosolvable topology on G, but it is not necessarily its full prosolvable topology (although in some cases it may be).

Next we describe some basic properties of the pro-$\mathcal{C}$ topology of a group G. Recall that the core H_G of H in G is the intersection of all conjugates of H in G. Observe that if $H \leq_f G$, then H has only finitely many conjugates; so,

$$H_G = \bigcap_{g \in G} H^g \triangleleft_f G.$$

Lemma 3.1.2 *Let $\mathcal{C}$ be a formation of finite groups. Assume that G is an abstract group and let $H \leq_f G$. Then*

(a) *H is open in the pro-$\mathcal{C}$ topology of G if and only if $G/H_G \in \mathcal{C}$.*
(b) *H is closed in the pro-$\mathcal{C}$ topology of G if and only if H is the intersection of open subgroups of G.*

Proof. (a) If $G/H_G \in \mathcal{C}$, then H_G is open; hence so is H. Conversely, if H is open, then so is every conjugate H^g of H in G; moreover, $H \leq_f G$, and so H has only finitely many conjugates. Therefore, H_G is open. Hence there exists some $N \triangleleft_f G$ with $G/N \in \mathcal{C}$ and $N \leq H_G$. Then there is an epimorphism $G/N \longrightarrow G/H_G$; thus $G/H_G \in \mathcal{C}$.

(b) Since an open subgroup has finite index, it is necessarily closed; therefore the intersection of open subgroups is closed. Conversely, assume H is a closed subgroup of G, and let $x \in G - H$. Then there exists some $N \in \mathcal{N}_{\mathcal{C}}(G)$ such that $xN \cap H = \emptyset$. Hence $x \notin HN$; so

$$H = \bigcap_{N \in \mathcal{N}_{\mathcal{C}}(G)} HN.$$

Since HN is open, the result follows. □

Example 3.1.3 Let $\mathcal{C}$ be a formation of finite groups, and assume that the group G is residually $\mathcal{C}$. If $H \leq G$, the pro-$\mathcal{C}$ topology of G induces on H a pro-$\mathcal{C}$ topology, but this is not necessarily the full pro-$\mathcal{C}$ topology of H, as the following examples show.

(1) Assume that $\mathcal{C}$ is the formation of all finite groups, $G = F$ is a free group of rank 2, and $H = F'$ the commutator subgroup of F. It is known that F' is a free group of countably infinite rank (cf. Magnus, Karras and Solitar [1966]). Let $\mathcal{I}$ be the topology induced on F' by the profinite topology of

F. It is plain that there are only countably many open subgroups in $\mathcal{I}$, while the profinite topology of F' has uncountably many open subgroups.

(2) Let $G = \langle a, b \mid b^2 = 1, bab = a^{-1}\rangle$ be the infinite dihedral group, and let $H = \langle a \rangle$. Then the pronilpotent topology of G induces on H only its pro-2 topology.

Next we indicate some cases where the induced pro-$\mathcal{C}$ topology on a subgroup coincides with the full pro-$\mathcal{C}$ topology of the subgroup.

Lemma 3.1.4

(a) *Let $\mathcal{C}$ be an extension closed variety of finite groups. Let H be a subgroup of G, open in the pro-$\mathcal{C}$ topology of G. Then the pro-$\mathcal{C}$ topology of G induces on H its full pro-$\mathcal{C}$ topology.*

(b) *Let $\mathcal{C}$ be an NE-formation of finite groups. Let H be a normal subgroup of G, open in the pro-$\mathcal{C}$ topology of G. Then the pro-$\mathcal{C}$ topology of G induces on H its full pro-$\mathcal{C}$ topology.*

Proof. (a) It suffices to show that if $N \lhd H$ and $H/N \in \mathcal{C}$, then there exists some $M \lhd G$ such that $G/M \in \mathcal{C}$ and $M \leq N$. We claim that we may take $M = N_G$, the core of N in G. Observe that if we put $K = H_G \cap N$, then $H/K \leq H/H_G \times H/N$, and hence $H/K \in \mathcal{C}$. Choose $g_1, \ldots, g_r \in G$ so that $K_G = \bigcap_{i=1}^r K^{g_i}$. Then $K^{g_i} \lhd H_G$ and $H_G/K^{g_i} \in \mathcal{C}$. Now, $H_G/K_G \leq H_G/K^{g_1} \times \cdots \times H_G/K^{g_r}$; and hence $H_G/K_G \in \mathcal{C}$. Thus the extension G/K_G of H_G/K_G by G/H_G belongs to $\mathcal{C}$. Finally, note that $N_G = K_G$, so that we can take $M = N_G$, as asserted.

(b) Let $N \lhd H$ with $H/N \in \mathcal{C}$. Choose $g_1, \ldots, g_r \in G$ so that $N_G = \bigcap_{i=1}^r N^{g_i}$. We claim that $H/N_G \in \mathcal{C}$. Note first that $H/N^{g_1} \cong H/N \in \mathcal{C}$. Moreover $N^{g_1}/N^{g_1} \cap N \cong N^{g_1}N/N \lhd H/N$; hence $N^{g_1}/N^{g_1} \cap N \in \mathcal{C}$, since $\mathcal{C}$ is closed under taking normal subgroups. It follows from the exactness of

$$1 \longrightarrow N^{g_1}/N^{g_1} \cap N \longrightarrow H/N^{g_1} \cap N \longrightarrow H/N^{g_1} \longrightarrow 1$$

that $H/N^{g_1} \cap N \in \mathcal{C}$, because $\mathcal{C}$ is also extension closed. The claim is now clear by induction. Next, observe that $G/H \in \mathcal{C}$, since H is open in the topology of G (see Lemma 3.1.2). Hence from the exactness of

$$1 \longrightarrow H/N_G \longrightarrow G/N_G \longrightarrow G/H \longrightarrow 1$$

we deduce that $G/N_G \in \mathcal{C}$. Consequently N_G, and thus N, are open in the pro-$\mathcal{C}$ topology of G. □

Lemma 3.1.5 *Let $\mathcal{C}$ be a variety of finite groups. Let $G = K \rtimes H$ be a semidirect product of the group K by the group H. Then*

(a) *The pro-$\mathcal{C}$ topology of G induces on H its full pro-$\mathcal{C}$ topology.*

(b) *Assume, in addition, that G is residually $\mathcal{C}$. Then H is closed in the pro-$\mathcal{C}$ topology of G.*

Proof. (a) Since $\mathcal{C}$ is subgroup closed, the pro-$\mathcal{C}$ topology of H is finer than the topology induced from G. Conversely, let $N \triangleleft_f H$ with $H/N \in \mathcal{C}$. Then $KN \triangleleft_f G$ and $G/KN \in \mathcal{C}$, since $G/KN \cong H/N$. Next note that $KN \cap H = N$.

(b) Consider the continuous maps

$$G \overset{\iota}{\underset{\varphi}{\rightrightarrows}} G,$$

where ι is the identity, $\varphi(kh) = h$ $(k \in K, h \in H)$, and G is assumed to have the pro-$\mathcal{C}$ topology. Then $H = \{g \in G \mid \iota(g) = \varphi(g)\}$. Hence H is closed, since the topology of G is Hausdorff. □

Corollary 3.1.6 *Let $\mathcal{C}$ be a variety of finite groups. Let $G = L * H$ be a free product of groups. Then*

(a) *The pro-$\mathcal{C}$ topology of G induces on H its full pro-$\mathcal{C}$ topology.*
(b) *Assume, in addition, that G is residually $\mathcal{C}$. Then H is closed in the pro-$\mathcal{C}$ topology of G.*

Proof. Denote by K the normal closure of L in G. Then $G = K \rtimes H$. Hence the results follow from the lemma above. □

3.2 The Pro-$\mathcal{C}$ Completion

Let G be a group and let $\mathcal{N}$ be a nonempty collection of normal subgroups of finite index of G filtered from below. Consider the topology on G determined by $\mathcal{N}$ as indicated in Section 3.1. The *completion* of G with respect to this topology is

$$\mathcal{K}_{\mathcal{N}}(G) = \varprojlim_{N \in \mathcal{N}} G/N.$$

Then $\mathcal{K}_{\mathcal{N}}(G)$ is a profinite group, and there exists a natural continuous homomorphism

$$\iota = \iota_{\mathcal{N}} : G \longrightarrow \mathcal{K}_{\mathcal{N}}(G),$$

induced by the epimorphisms $G \longrightarrow G/N$ $(N \in \mathcal{N})$. Namely, $\iota(g) = (gN)_{N \in \mathcal{N}}$, for each $g \in G$. Observe that $\iota(G)$ is a dense subset of $\mathcal{K}_{\mathcal{N}}(G)$ (see Lemma 1.1.7). The map ι is injective if and only if $\bigcap_{N \in \mathcal{N}} N = 1$.

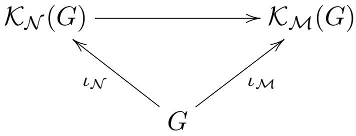
Suppose that $\mathcal{M}$ is a subcollection of $\mathcal{N}$ which is also filtered from below. Then the epimorphisms

$$\mathcal{K}_{\mathcal{N}}(G) \longrightarrow G/M \quad (M \in \mathcal{M})$$

induce a continuous epimorphism

$$\mathcal{K}_{\mathcal{N}}(G) \longrightarrow \mathcal{K}_{\mathcal{M}}(G)$$

that makes the following diagram commutative

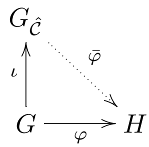


Let $\mathcal{C}$ be a formation of finite groups and let $\mathcal{N}_\mathcal{C}(G)$ be the collection of normal subgroups of G defined in (1). Then the completion $\mathcal{K}_{\mathcal{N}_\mathcal{C}(G)}(G)$ is just the pro-$\mathcal{C}$ completion of G as defined in Example 2.1.6. In this case we usually denote the completion $\mathcal{K}_{\mathcal{N}_\mathcal{C}(G)}(G)$ by $\mathcal{K}_\mathcal{C}(G)$ or by $G_{\hat{\mathcal{C}}}$. If $\mathcal{C}$ is the formation of all finite p-groups, for a fixed prime number p, then one often uses the notation $G_{\hat{p}}$ for the corresponding completion. We shall reserve the notation $\widehat{G}$ for the profinite completion of G, i.e., the completion $G_{\hat{\mathcal{C}}}$, where $\mathcal{C}$ is the formation of all finite groups.

Lemma 3.2.1 *Let $\mathcal{C}$ be a formation of finite groups and let G be a group. Then the pro-$\mathcal{C}$ completion $G_{\hat{\mathcal{C}}}$ of a group G is characterized as follows. $G_{\hat{\mathcal{C}}}$ is a pro-$\mathcal{C}$ group together with a continuous homomorphism*

$$\iota : G \longrightarrow G_{\hat{\mathcal{C}}}$$

onto a dense subgroup of $G_{\hat{\mathcal{C}}}$, where G is endowed with the pro-$\mathcal{C}$ topology, and the following universal property is satisfied:



whenever H is a pro-$\mathcal{C}$ group and $\varphi : G \longrightarrow H$ a continuous homomorphism, there exists a continuous homomorphism $\bar{\varphi} : G_{\hat{\mathcal{C}}} \longrightarrow H$ such that $\bar{\varphi}\iota = \varphi$. Moreover, it suffices to check this property for $H \in \mathcal{C}$.

Proof. We verify first that the completion $G_{\hat{\mathcal{C}}}$, as defined above, together with the map ι satisfy the indicated universal property. Let $\varphi : G \longrightarrow H$ be a continuous homomorphism into a pro-$\mathcal{C}$ group H. Set $\mathcal{U} = \{U \mid U \triangleleft_o H\}$ and let $U \in \mathcal{U}$. Define $N_U = \varphi^{-1}(U)$. Then there is a composition of natural continuous homomorphisms

$$\varphi_U : G_{\hat{\mathcal{C}}} \longrightarrow G/N_U \longrightarrow H/U.$$

Then the maps φ_U $(U \in \mathcal{U})$ are compatible. Hence they define a continuous homomorphism

$$\bar{\varphi} : G_{\hat{\mathcal{C}}} \longrightarrow \varprojlim_{U \in \mathcal{U}} H/U = H$$

such that $\varphi_{UV}\bar{\varphi} = \varphi_V$ whenever $U, V \in \mathcal{U}$ and $U \leq V$, where

$$\varphi_{UV} : H/U \longrightarrow H/V$$

is the canonical epimorphism. Then one verifies without difficulty that $\bar{\varphi}\iota = \varphi$.

The fact that this universal property characterizes the completion follows a standard argument that we only sketch. Say that K is a pro-$\mathcal{C}$ group and

$$\kappa : G \longrightarrow K$$

is a continuous homomorphism whose image is dense in K. Assume that the pair (K, κ) also satisfies the required universal property. Then there exist continuous homomorphisms $\bar{\iota} : K \longrightarrow G_{\hat{\mathcal{C}}}$ and $\bar{\kappa} : G_{\hat{\mathcal{C}}} \longrightarrow K$ such that $\bar{\iota}\kappa = \iota$ and $\bar{\kappa}\iota = \kappa$. Since $\iota(G)$ and $\kappa(G)$ are dense in $G_{\hat{\mathcal{C}}}$ and K, respectively, it follows that $\bar{\iota}\bar{\kappa}$ and $\bar{\kappa}\bar{\iota}$ are the identity maps on $G_{\hat{\mathcal{C}}}$ and K, respectively. Therefore $\bar{\iota}$ is a continuous isomorphism.

The last statement of the lemma is clear from the construction of $\bar{\varphi}$ in the first part of the proof. □

Proposition 3.2.2 *Let $\mathcal{C}$ be a formation and assume that G is a residually $\mathcal{C}$ group. Identify G with its image in its pro-$\mathcal{C}$ completion $G_{\hat{\mathcal{C}}}$. Let $\bar{X}$ denote the closure in $G_{\hat{\mathcal{C}}}$ of a subset X of G.*

(a) *Let*

$$\Phi : \{N \mid N \leq_o G\} \longrightarrow \{U \mid U \leq_o G_{\hat{\mathcal{C}}}\}$$

be the mapping that assigns to each open subgroup H of G its closure $\bar{H}$ in $G_{\hat{\mathcal{C}}}$. Then Φ is a one-to-one correspondence between the set of all open subgroups H in the pro-$\mathcal{C}$ topology of G and the set of all open subgroups of $G_{\hat{\mathcal{C}}}$. The inverse of this mapping is

$$U \longmapsto U \cap G;$$

in particular, $\overline{U \cap G} = U$ if $U \leq_o G_{\hat{\mathcal{C}}}$.

(b) *The map Φ sends normal subgroups to normal subgroups.*

(c) *The topology of $G_{\hat{\mathcal{C}}}$ induces on G its full pro-$\mathcal{C}$ topology.*

(d) *If $H, K \in \{N \mid N \leq_o G\}$ and $H \leq K$, then $[K : H] = [\bar{K} : \bar{H}]$; moreover, if in addition $H \triangleleft K$, then $K/H \cong \bar{K}/\bar{H}$.*

(e) *Φ is an isomorphism of lattices, i.e., if $H, K \in \{N \mid N \leq_o G\}$, then $\overline{H \cap K} = \bar{H} \cap \bar{K}$ and $\overline{\langle H, K \rangle} = \langle \bar{H}, \bar{K} \rangle$.*

Proof. Denote by $\mathcal{N}$, as usual, the collection of all open normal subgroups of G in its pro-$\mathcal{C}$ topology, i.e., the collection of those normal subgroups of G such that $G/N \in \mathcal{C}$.

(a) Let U be an open subgroup of $G_{\hat{\mathcal{C}}}$. Since G is dense in $G_{\hat{\mathcal{C}}}$, it follows that $G \cap U$ is dense in U. Hence $\overline{U \cap G} = U$. Conversely, assume that H is an open subgroup of G (in the pro-$\mathcal{C}$ topology of G). We must show that $H = G \cap \overline{H}$; plainly, $H \leq G \cap \overline{H}$. Let $g \in G \cap \overline{H}$. Recall that G is embedded in $G_{\hat{\mathcal{C}}}$ via the identification

$$g \mapsto (gN) \in G_{\hat{\mathcal{C}}} = \varprojlim_{\mathcal{N}} G/N.$$

Now, according to Corollary 1.1.8,

$$\overline{H} = \varprojlim_{N \in \mathcal{N}} HN/N.$$

So $g \in HN$ for every $N \in \mathcal{N}$. Since $H_G \in \mathcal{N}$, it follows that $g \in HH_G = H$. Thus $H \geq G \cap \overline{H}$, as desired.

(b) If $H \triangleleft G$, then $HN/N \triangleleft G/N$ for each $N \in \mathcal{N}$; hence $\bar{H} \triangleleft G_{\hat{\mathcal{C}}}$. Conversely, if $U \triangleleft_o G_{\hat{\mathcal{C}}}$ then $U \cap G \triangleleft G$; therefore the function Φ maps normal subgroups to normal subgroups.

(c) This follows from (a).

(d) It suffices to show that if $H \in \{N \mid N \leq_o G\}$, then $[G : H] = [G_{\hat{\mathcal{C}}} : \bar{H}]$. Say $n = [G_{\hat{\mathcal{C}}} : \bar{H}]$; since G is dense in $G_{\hat{\mathcal{C}}}$, we deduce that $G\bar{H} = G_{\hat{\mathcal{C}}}$. Let $t_1, \dots, t_n \in G$ be a left transversal of $\bar{H}$ in $G_{\hat{\mathcal{C}}}$. Then we have a disjoint union

$$G_{\hat{\mathcal{C}}} = t_1\bar{H} \cupdot \cdots \cupdot t_n\bar{H}.$$

If $t \in G$, it follows from part (a) that $t\bar{H} \cap G = tH$; therefore,

$$G = (t_1\overline{H} \cupdot \cdots \cupdot t_n\overline{H}) \cap G = t_1H \cupdot \cdots \cupdot t_nH;$$

thus $n = [G : H]$.

Now, if $H \triangleleft K$ and $H, K \in \{N \mid N \leq_o G\}$, the natural homomorphism $K \longrightarrow \bar{K}/\bar{H}$ has kernel $K \cap \bar{H} = H$. From $[\bar{K} : \bar{H}] = [K : H]$, we infer that the induced homomorphism $K/H \longrightarrow \bar{K}/\bar{H}$ is an isomorphism.

(e) This follows from (a) and (d). □

The Completion Functor

Let $\varphi : G \longrightarrow H$ be a group homomorphism. We wish to define canonically a corresponding continuous homomorphism

$$G_{\hat{\mathcal{C}}} \longrightarrow H_{\hat{\mathcal{C}}},$$

whenever possible. The idea is to define compatible continuous homomorphisms $G \longrightarrow H/N$ ($N \in \mathcal{N}_{\mathcal{C}}(H)$), and then use Lemma 3.2.1. We shall do this in a completely explicit manner.

Consider the collection $\mathcal{M} = \{\varphi^{-1}(N) \mid N \in \mathcal{N}_{\mathcal{C}}(H)\}$ of normal subgroups of G. Clearly $\mathcal{M}$ is filtered from below. Assume that

$$\varphi^{-1}(N) \in \mathcal{N}_{\mathcal{C}}(G) \quad \text{for all } N \in \mathcal{N}_{\mathcal{C}}(H). \tag{3}$$

Note that this is the case if, for example, one of the following conditions is satisfied

– $\mathcal{C}$ is a variety of finite groups;
– $\mathcal{C}$ is a formation of finite groups and φ is an epimorphism;
– $\mathcal{C}$ is a formation of finite groups closed under taking normal subgroups, and $\varphi(G) \triangleleft H$.

Then $\mathcal{M}$ determines a pro-$\mathcal{C}$ topology on G. For each $N \in \mathcal{N}_{\mathcal{C}}(H)$ one has a composition of natural homomorphisms

$$\mathcal{K}_{\mathcal{M}}(G) \longrightarrow G/\varphi^{-1}(N) \longrightarrow \varphi(G)/N \cap \varphi(G) \hookrightarrow H/N.$$

These maps, in turn, induce continuous homomorphisms

$$\mathcal{K}_{\mathcal{M}}(G) \stackrel{\varphi_1}{\to} \varprojlim_{N \in \mathcal{N}} G/\varphi^{-1}(N) \stackrel{\varphi_2}{\to} \varprojlim_{N \in \mathcal{N}} \varphi(G)/N \cap \varphi(G) \stackrel{\varphi_3}{\to} \varprojlim_{N \in \mathcal{N}} H/N = H_{\hat{\mathcal{C}}},$$

where $\mathcal{N} = \mathcal{N}_{\mathcal{C}}(H)$, φ_1 is an epimorphism, φ_2 an isomorphism, and φ_3 an inclusion (see Proposition 2.2.4). On the other hand, since $\mathcal{M}$ is a subset of $\mathcal{N}_{\mathcal{C}}(G)$, there exists an epimorphism $G_{\hat{\mathcal{C}}} \longrightarrow \mathcal{K}_{\mathcal{M}}(G)$ as indicated above. Define

$$\varphi_{\hat{\mathcal{C}}} = \mathcal{K}_{\mathcal{C}}(\varphi) : G_{\hat{\mathcal{C}}} \longrightarrow H_{\hat{\mathcal{C}}}$$

to be the composition homomorphism

$$G_{\hat{\mathcal{C}}} \longrightarrow \mathcal{K}_{\mathcal{M}}(G) \longrightarrow H_{\hat{\mathcal{C}}}.$$

From now on, whenever we write $\varphi_{\hat{\mathcal{C}}}$, it is assumed that this map is defined, i.e., that condition (3) is satisfied.

It is plain that if $\mathrm{id} : G \longrightarrow G$ is the identity homomorphism, then $\mathrm{id}_{\hat{\mathcal{C}}} : G_{\hat{\mathcal{C}}} \longrightarrow G_{\hat{\mathcal{C}}}$ is the identity homomorphism. Furthermore, if $\varphi : G \longrightarrow H$ and $\psi : H \longrightarrow K$ are group homomorphisms, then $(\psi\varphi)_{\hat{\mathcal{C}}} = \psi_{\hat{\mathcal{C}}}\varphi_{\hat{\mathcal{C}}}$, whenever the maps $(\psi\varphi)_{\hat{\mathcal{C}}}$, $\psi_{\hat{\mathcal{C}}}$ and $\varphi_{\hat{\mathcal{C}}}$ are defined. Therefore we have, in particular,

Lemma 3.2.3 *Let $\mathcal{C}$ be a variety of finite groups. Then, pro-$\mathcal{C}$ completion $(-)_{\hat{\mathcal{C}}}$ is a functor from the category of abstract groups to the category of pro-$\mathcal{C}$ groups and continuous homomorphisms.*

Let $\varphi : G \longrightarrow H$ be a group homomorphism. It follows from the definition of $\varphi_{\hat{\mathcal{C}}}$ that the diagram

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \downarrow{\scriptstyle\iota} & & \downarrow{\scriptstyle\iota} \\ G_{\hat{\mathcal{C}}} & \xrightarrow[\varphi_{\hat{\mathcal{C}}}]{} & H_{\hat{\mathcal{C}}} \end{array}$$

commutes. Since $\iota(H)$ is dense in $H_{\hat{\mathcal{C}}}$, one deduces that $(\iota\varphi)(G)$ is dense in $\varphi_{\hat{\mathcal{C}}}(G_{\hat{\mathcal{C}}})$. On the other hand $\varphi_{\hat{\mathcal{C}}}(G_{\hat{\mathcal{C}}})$ is closed by the compactness of $G_{\hat{\mathcal{C}}}$. Therefore, $\varphi_{\hat{\mathcal{C}}}(G_{\hat{\mathcal{C}}})$ is the closure of $(\iota\varphi)(G)$ in $H_{\hat{\mathcal{C}}}$. We record this in the following lemma.

Lemma 3.2.4 *Let $\mathcal{C}$ be a formation of finite groups. Let $\varphi : G \longrightarrow H$ be a homomorphism of groups and assume that $\varphi_{\hat{\mathcal{C}}} : G_{\hat{\mathcal{C}}} \longrightarrow H_{\hat{\mathcal{C}}}$ is defined. Then*

$$\varphi_{\hat{\mathcal{C}}}(G_{\hat{\mathcal{C}}}) = \overline{(\iota\varphi)(G)},$$

where $\overline{(\iota\varphi)(G)}$ denotes the closure of $(\iota\varphi)(G)$ in $H_{\hat{\mathcal{C}}}$.

Proposition 3.2.5 *Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups. Then the functor $(-)_{\hat{\mathcal{C}}}$ is right exact, that is, if*

$$1 \longrightarrow K \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$$

is an exact sequence of groups, then

$$K_{\hat{\mathcal{C}}} \xrightarrow{\varphi_{\hat{\mathcal{C}}}} G_{\hat{\mathcal{C}}} \xrightarrow{\psi_{\hat{\mathcal{C}}}} H_{\hat{\mathcal{C}}} \longrightarrow 1$$

is an exact sequence of pro-$\mathcal{C}$ groups.

Proof. Let $\mathcal{N} = \mathcal{N}_{\mathcal{C}}(G)$. Then we get in a natural way a corresponding exact sequence of inverse systems (indexed by $\mathcal{N}$)

$$\{K/\varphi^{-1}(N) \mid N \in \mathcal{N}\} \xrightarrow{\tilde{\varphi}} \{G/N \mid N \in \mathcal{N}\} \xrightarrow{\tilde{\psi}} \{H/\psi(N) \mid N \in \mathcal{N}\} \longrightarrow 1.$$

Observe that

$$\varprojlim_{N\in\mathcal{N}} G/N = G_{\hat{\mathcal{C}}}, \qquad \varprojlim_{N\in\mathcal{N}} H/\psi(N) = H_{\hat{\mathcal{C}}}, \quad \text{and} \quad \varprojlim \tilde{\psi} = \psi_{\hat{\mathcal{C}}}.$$

On the other hand, $\varphi_{\hat{\mathcal{C}}}$ is the composition of the epimorphism

$$K_{\hat{\mathcal{C}}} \longrightarrow \varprojlim_{N\in\mathcal{N}} K/\varphi^{-1}(N)$$

and $\varprojlim \tilde{\varphi}$. Our result follows now from the exactness of the functor $\varprojlim$ (see Proposition 2.2.4). □

A necessary and sufficient condition for the completion functor $(-)_{\hat{\mathcal{C}}}$ to preserve an injection $\iota : K \longrightarrow G$ is stated in the next lemma.

Lemma 3.2.6 *Let $\mathcal{C}$ be a variety (respectively, a formation closed under taking normal subgroups) of finite groups. Assume that $K \leq G$ (respectively, $K \triangleleft G$), and let $\iota : K \longrightarrow G$ denote the inclusion map. Then*

$$\iota_{\hat{\mathcal{C}}} : K_{\hat{\mathcal{C}}} \longrightarrow G_{\hat{\mathcal{C}}}$$

is injective if and only if the pro-$\mathcal{C}$ topology of G induces on K its full pro-$\mathcal{C}$ topology.

Proof. Let $N \triangleleft_f G$ be such that $G/N \in \mathcal{C}$. Then $K/K \cap N \in \mathcal{C}$. Therefore, there exists a natural epimorphism $K_{\hat{\mathcal{C}}} \longrightarrow K/K \cap N$. The map $\iota_{\hat{\mathcal{C}}}$ is the composition

$$K_{\hat{\mathcal{C}}} \longrightarrow \varprojlim_{N \in \mathcal{N}_{\mathcal{C}}(G)} K/K \cap N \longrightarrow \varprojlim_{N \in \mathcal{N}_{\mathcal{C}}(G)} G/N = G_{\hat{\mathcal{C}}}.$$

The map on the right is always an injection. Hence $\iota_{\hat{\mathcal{C}}}$ is an injection if and only if the epimorphism

$$\rho : K_{\hat{\mathcal{C}}} \longrightarrow \varprojlim_{N \in \mathcal{N}_{\mathcal{C}}(G)} K/K \cap N$$

is injective, i.e., an isomorphism. If the pro-$\mathcal{C}$ topology of G induces on K its full pro-$\mathcal{C}$ topology, then the collection of normal subgroups

$$\{K \cap N \mid N \in \mathcal{N}_{\mathcal{C}}(G)\}$$

is cofinal in $\mathcal{N}_{\mathcal{C}}(K)$; hence ρ is an isomorphism (see Lemma 1.1.9). Conversely, if ρ is an isomorphism, then $\{K \cap N \mid N \in \mathcal{N}_{\mathcal{C}}(G)\}$ is a fundamental system of neighborhoods of 1 in K (see Lemma 2.1.1); in other words, the pro-$\mathcal{C}$ topology of G induces on K its full pro-$\mathcal{C}$ topology. □

In the next result, we indicate how possibly different groups could have the same completions.

Theorem 3.2.7 *Let $\mathcal{C}$ be a formation of finite groups. Let G_1, G_2 be groups. Denote by $\mathcal{U}_i$ the collection of all normal subgroups U of G_i with $G_i/U \in \mathcal{C}$ $(i = 1, 2)$. Assume that*

(a) *For each natural number n, there exist only finitely many $U \in \mathcal{U}_i$ such that $[G_i : U] \leq n$; and*
(b) $\{G_1/U \mid U \in \mathcal{U}_1\} = \{G_2/V \mid V \in \mathcal{U}_2\}$.

Then

$$\varprojlim_{U \in \mathcal{U}_1} G_1/U \cong \varprojlim_{V \in \mathcal{U}_2} G_2/V.$$

Proof. For each $n \in \mathbf{N}$, let

$$U_n = \bigcap \{U \mid U \in \mathcal{U}_1, [G_1 : U] \leq n\} \quad \text{and}$$
$$V_n = \bigcap \{U \mid U \in \mathcal{U}_2, [G_2 : U] \leq n\}.$$

Then $U_n \in \mathcal{U}_1$ and $V_n \in \mathcal{U}_2$. So there exists some $K \in \mathcal{U}_1$ with $G_1/K \cong G_2/V_n$. It follows from (b) that K is the intersection of groups $U \in \mathcal{U}_1$ with $[G : U] \leq n$; therefore $K \geq U_n$. Hence, $|G_1/U_n| \geq |G_2/V_n|$. By symmetry $|G_1/U_n| \leq |G_2/V_n|$. Thus $G_1/U_n \cong G_2/V_n$. Let X_n be the set of all isomorphisms from G_1/U_n to G_2/V_n. Observe that if $\sigma_{n+1} \in X_{n+1}$, then $\sigma(U_n/U_{n+1}) = V_n/V_{n+1}$; hence σ_{n+1} induces an isomorphism

$$\sigma_n : G_1/U_n \longrightarrow G_2/V_n.$$

Denote by

$$\varphi_{n+1,n} : X_{n+1} \longrightarrow X_n$$

the map defined by $\sigma_{n+1} \mapsto \sigma_n$. Then $\{X_n, \varphi_{n+1,n}\}$ is an inverse system of finite nonempty sets. Hence there exists some $(\sigma_n) \in \varprojlim X_n$ (see Proposition 1.1.4). On the other hand,

$$\{G_1/U_n\}_{n=1}^{\infty} \quad \text{and} \quad \{G_2/V_n\}_{n=1}^{\infty}$$

are in a natural way inverse systems of groups; furthermore, $\{\sigma_n\}_{n=1}^{\infty}$ is an isomorphism of these systems. Finally, it follows from Lemma 1.1.9 that

$$\varprojlim_{U \in \mathcal{U}_1} G_1/U \cong \varprojlim_{n} G_1/U_n \cong \varprojlim_{n} G_2/V_n \cong \varprojlim_{V \in \mathcal{U}_2} G_2/V$$

since $\{G_1/U_n\}_{n=1}^{\infty}$ and $\{G_2/V_n\}_{n=1}^{\infty}$ are cofinal subsystems of $\{G_1/U \mid U \in \mathcal{U}_1\}$ and $\{G_2/V \mid V \in \mathcal{U}_2\}$, respectively. □

Corollary 3.2.8 *Let G_1, G_2 be finitely generated abstract groups with the same finite quotients, then $\widehat{G}_1 \cong \widehat{G}_2$.*

Using a slight variation of the argument in Theorem 3.2.7, we obtain

Theorem 3.2.9 *Let G_1 be a finitely generated profinite group and let G_2 be any profinite group. Assume that G_1 and G_2 have the same finite quotients, i.e., $\{G_1/U \mid U \triangleleft_o G_1\} = \{G_2/V \mid V \triangleleft_o G_2\}$. Then $G_1 \cong G_2$.*

3.3 Free Pro-$\mathcal{C}$ Groups

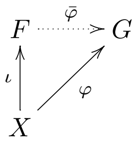
Unless otherwise specified, throughout this section $\mathcal{C}$ denotes a formation of finite groups, i.e., we assume that $\mathcal{C}$ is a class of finite groups closed under taking quotient groups and finite subdirect products; moreover, we assume that $\mathcal{C}$ contains a group of order at least two.

A topological space X with a distinguished point $*$ is called a *pointed space*. We shall denote such a space by $(X, *)$. Sometimes it is convenient to think of a profinite group as a pointed space with distinguished point 1. A mapping of pointed spaces

$$\varphi : (X, *) \longrightarrow (X', *')$$

is simply a continuous mapping from X into X' such that $\varphi(*) = *'$.

Let X be a profinite space, F a pro-$\mathcal{C}$ group and $\iota : X \longrightarrow F$ a continuous mapping such that $F = \overline{\langle \iota(X) \rangle}$. We say that (F, ι) is a *free pro-$\mathcal{C}$ group* on the profinite space X or, simply, F is a free pro-$\mathcal{C}$ group on X, if the following universal property is satisfied:



whenever $\varphi : X \longrightarrow G$ is a continuous mapping into a pro-$\mathcal{C}$ group G such that $\varphi(X)$ generates G, then there exists a (necessarily unique) continuous homomorphism $\bar{\varphi} : F \longrightarrow G$ such that the above diagram commutes: $\bar{\varphi}\iota = \varphi$.

One defines a *free pro-$\mathcal{C}$ group* on a pointed profinite space $(X, *)$ in an analogous manner: one simply assumes in the description of the universal property that the maps involved are maps of pointed spaces.

Note that if the profinite space X is empty, then a free pro-$\mathcal{C}$ group on X must be the trivial group. If X contains exactly one element and $\mathcal{C}$ does not contain nontrivial cyclic groups, then the free pro-$\mathcal{C}$ group on the profinite space X is the trivial group. Similarly, if a profinite pointed space $(X, *)$ contains exactly one point, then free pro-$\mathcal{C}$ group on the pointed space $(X, *)$ is the trivial group. If $(X, *)$ has exactly two points and $\mathcal{C}$ does not contain nontrivial cyclic groups, then a free pro-$\mathcal{C}$ group on the pointed space $(X, *)$ is the trivial group.

To avoid trivial counterexamples to some of the statements in this chapter, from now on we shall tacitly assume that if $\mathcal{C}$ does not contain nontrivial cyclic groups, then we only consider free pro-$\mathcal{C}$ groups on profinite spaces X that are either empty or of cardinality at least 2 (*respectively, we only consider free pro-$\mathcal{C}$ groups on profinite pointed spaces* $(X, *)$ *such that either* $|X| = 1$ *or* $|X| \geq 3$).

Observe that one needs to test the universal property in the definition of free pro-$\mathcal{C}$ groups only for finite groups G in $\mathcal{C}$, for then it holds automatically for any pro-$\mathcal{C}$ group G, since G is an inverse limit of groups in $\mathcal{C}$.

From the universal definition, one deduces in a standard manner that if a free pro-$\mathcal{C}$ group exists, then it is unique. We shall denote the free pro-$\mathcal{C}$ group on a profinite space X by $F_{\mathcal{C}}(X)$, and the free pro-$\mathcal{C}$ group on a pointed profinite space $(X, *)$ by $F_{\mathcal{C}}(X, *)$.

Lemma 3.3.1 *Let* (F, ι) *be a free pro-$\mathcal{C}$ group on the profinite space* X (*respectively, a free pro-$\mathcal{C}$ group on the pointed profinite space* $(X, *)$), *then the mapping* ι *is an injection and* $1 \notin \iota(X)$ (*respectively,* ι *is an injection*).

Proof. We give a proof for the nonpointed case. If $X = \{x\}$ has cardinality 1, then, by our standing assumptions, there exists a nontrivial finite cyclic group $\langle a \rangle \in \mathcal{C}$. Let $\varphi : X \longrightarrow \langle a \rangle$ be given by $\varphi(x) = a$. Let $\bar{\varphi} : F \longrightarrow \langle a \rangle$ be the continuous homomorphism such that $\varphi(\iota(x)) = a$. It follows that $\iota(x) \neq 1$. Assume now that $|X| \geq 2$. Consider the set $\mathcal{R}$ of all open equivalence relations R on X. According to Theorem 1.1.12, the clopen subsets of X form a base for the topology of X. Therefore, if $x \neq y$ are points of X, there exists $R \in \mathcal{R}$ such that $xR \neq yR$. Let $G \in \mathcal{C}$ be generated by two distinct nontrivial elements, say, a and b (such a group exists: indeed, let $H \in \mathcal{C}$ be a nontrivial group; let S be a quotient of H such that S is a simple group; if S is nonabelian, then it is a two generator group, by the classification of finite simple groups, and then put $G = S$; while if S is cyclic, take $G = S \times S$). Consider the continuous mapping

$$\psi : X \xrightarrow{\psi_R} X/R \xrightarrow{\rho} G$$

where ψ_R is the canonical quotient map, and ρ any map such that $\rho(xR) = a$ and $\rho(yR) = b$. Since ψ is continuous, there exists a corresponding continuous homomorphism $\bar{\psi} : F \longrightarrow G$ such that $\bar{\psi}\iota = \psi$. It follows that $1 \neq \iota(x) \neq \iota(y) \neq 1$, and so ι is one-to-one and $1 \notin \iota(X)$. □

Next we show the existence of free pro-$\mathcal{C}$ groups.

Proposition 3.3.2 *For every profinite space X (respectively, pointed profinite space $(X, *)$), there exists a unique free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(X)$ on X (respectively, there exists a unique free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(X, *)$ on the pointed profinite space $(X, *)$).*

Proof. We leave the uniqueness to the reader. For the construction of $F_{\mathcal{C}}(X)$, let D be the abstract free group on the set X. Consider the following collection of subgroups of D

$$\mathcal{N} = \{N \triangleleft D \mid D/N \in \mathcal{C}; X \cap dN \text{ open in } X, \forall d \in D\}.$$

Observe that $\mathcal{N}$ is nonempty and filtered from below. Define $F_{\mathcal{C}}(X)$ to be the completion of D with respect to $\mathcal{N}$

$$F_{\mathcal{C}}(X) = \varprojlim_{N \in \mathcal{N}} D/N.$$

Let $\iota : X \longrightarrow F_{\mathcal{C}}(X)$ be the restriction to X of the natural homomorphism $D \longrightarrow F_{\mathcal{C}}(X)$. Remark that the composition of ι with each projection $F_{\mathcal{C}}(X) \longrightarrow D/N$, $N \in \mathcal{N}$, is continuous, and hence, so is ι. Next we show that $(F_{\mathcal{C}}(X), \iota)$ is a free pro-$\mathcal{C}$ group on X. Indeed, let $G \in \mathcal{C}$ and let $\varphi : X \longrightarrow G$ be a continuous map such that $G = \langle \varphi(X) \rangle$. Since D is a free abstract group on X, there exists a homomorphism (of abstract groups) $\varphi_1 : D \longrightarrow G$ that extends φ. In fact φ_1 is an epimorphism. Put $K = \mathrm{Ker}(\varphi_1)$. Then $K \in \mathcal{N}$. Therefore, we have a continuous homomorphism

$$\bar{\varphi} : F_{\mathcal{C}}(X) \longrightarrow D/K \longrightarrow G.$$

Then $\bar{\varphi}\iota = \varphi$.

The construction of $F_{\mathcal{C}}(X,*)$ is as follows: let $\tilde{D}$ be the abstract free group on the set $X-\{*\}$, and let

$$\tilde{\mathcal{N}}=\{N\triangleleft\tilde{D}\mid\tilde{D}/N\in\mathcal{C};(X-\{*\})\cap dN\text{ open in }X-\{*\},\forall d\in\tilde{D}\}.$$

Put

$$F_{\mathcal{C}}(X,*)=\varprojlim_{N\in\tilde{\mathcal{N}}}\tilde{D}/N.$$

Then one checks as above that $(F_{\mathcal{C}}(X,*),\iota)$ satisfies the universal property of a free pro-$\mathcal{C}$ group on the pointed profinite space $(X,*)$. □

We shall refer to the profinite space X (respectively, $(X,*)$) as a *topological basis* of $F_{\mathcal{C}}(X)$ (respectively, of $F_{\mathcal{C}}(X,*)$).

If X is a profinite space, one can associate with it a pointed profinite space $(X\,\dot\cup\,\{*\},*)$, by simply adding to X a new point $*$ and endowing $X\,\dot\cup\,\{*\}$ with the coproduct topology, i.e., $*$ is an isolated point in $X\,\dot\cup\,\{*\}$ and a subset Y of $X\,\dot\cup\,\{*\}$ is open if and only if $Y\cap X$ is open in X. Then one easily sees that $F_{\mathcal{C}}(X)=F_{\mathcal{C}}(X\,\dot\cup\,\{*\},*)$. Thus, we can think of a free pro-$\mathcal{C}$ group on a profinite space as particular instance of a free pro-$\mathcal{C}$ group on a pointed profinite space.

Exercise 3.3.3 Let $(X,*)$ be a pointed topological space, not necessarily profinite.

(a) Mimic the definition above to establish the concept of a free pro-$\mathcal{C}$ group $(F_{\mathcal{C}}(X,*),\iota)$ on the pointed space $(X,*)$. As a special case of the above definition, explain the concept of free pro-$\mathcal{C}$ group $(F_{\mathcal{C}}(X),\iota)$ on a topological space X.

(b) Define

$$(\check{X},*)=\varprojlim_{R\in\mathcal{R}}(X,*)/R,$$

where $\mathcal{R}$ is the collection of all closed equivalence relations R of X such that the quotient pointed space $(X,*)/R$ is finite and Hausdorff. Let $\tau:X\longrightarrow\check{X}$ be the natural mapping. Show that there exists a unique continuous mapping of pointed spaces $\tilde{\iota}:(\check{X},*)\longrightarrow F_{\mathcal{C}}(X,*)$ such that $\iota=\tilde{\iota}\tau$.

(c) Prove that $|\mathcal{R}|=\rho(\check{X})$, the cardinality of the collection of all clopen subsets of $\check{X}$.

(d) Show that $F_{\mathcal{C}}(X,*)$ is a free pro-$\mathcal{C}$ group on a pointed profinite space; specifically, prove that $(F_{\mathcal{C}}(X,*),\tilde{\iota})$ is the free pro-$\mathcal{C}$ group on the pointed profinite space $(\check{X},*)$.

Free Pro-$\mathcal{C}$ Group on a Set Converging to 1

If X is a set, we say that a map $\mu:X\longrightarrow G$ from X to a profinite group G *converges to* 1 if the subset $\mu(X)$ of G converges to 1, that is, if every open subgroup U of G contains all but a finite number of the elements of $\mu(X)$.

Assume now X to be a set, which we wish to view as a topological space with the discrete topology. Let $\bar{X} = X \cup \{*\}$ denote its one-point compactification (recall that, by definition, a subset T is open in $\bar{X}$ if either it is contained in X or $\{*\} \in T$ and $X - T$ is a finite set; see, e.g., Bourbaki [1989], I,9,8). Then $X \cup \{*\}$ is a profinite space. Observe that if X is a set and $X \cup \{*\}$ is its one-point compactification, then the map

$$X \hookrightarrow X \cup \{*\} \stackrel{\iota}{\longrightarrow} F_{\mathcal{C}}(X \cup \{*\}, *)$$

converges to 1. We shall still denote this map by ι.

To avoid trivial cases, from now on we shall assume that if $\mathcal{C}$ does not contain nontrivial cyclic groups, then $|X| \neq 2$.

Then (see Lemma 3.3.1) ι is a topological embedding, and we identify X with its image in $F_{\mathcal{C}}(X \cup \{*\}, *)$. The free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(X \cup \{*\}, *)$ on this pointed space $(X \cup \{*\}, *)$ plays a special role because, as we shall see later (Proposition 3.5.12), every free pro-$\mathcal{C}$ group on a (pointed) topological space is in fact a free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(X \cup \{*\}, *)$ on the one-point compactification space $(X \cup \{*\}, *)$ of some set X.

Let X be a set. By abuse of notation, we denote the free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(X \cup \{*\}, *)$ on the one-point compactification space $(X \cup \{*\}, *)$ of X, as $F_{\mathcal{C}}(X)$ rather than $F_{\mathcal{C}}(X \cup \{*\}, *)$. To avoid confusion, if X is a set, we refer to $F_{\mathcal{C}}(X)$ in that case as the *free pro-$\mathcal{C}$ group on the set X converging to* 1.* If, on the other hand, X (respectively, $(X, *)$) is a profinite space (respectively, a pointed profinite space), then $F_{\mathcal{C}}(X)$ (respectively, $F_{\mathcal{C}}(X, *)$) has a unique possible meaning, and we refer to it as the free pro-$\mathcal{C}$ group on X or on the space X (respectively, the free pro-$\mathcal{C}$ group on $(X, *)$ or on the pointed space $(X, *)$). If X is a finite subset of a profinite group, then X converges to 1; so in this case the meaning of $F_{\mathcal{C}}(X)$ is unambiguous, and we refer to it as the free pro-$\mathcal{C}$ group on X.

The following lemma gives a characterization of the free group on a set converging to 1 in terms of a universal property. We leave its easy proof to the reader (it follows immediately from the definition of free pro-$\mathcal{C}$ group on a pointed space in the special case where the pointed space is the one-point compactification of a discrete space).

Lemma 3.3.4 *The following properties characterize the free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(X)$ on the set X converging to* 1:

(a) *$F_{\mathcal{C}}(X)$ contains the set X as a subset converging to* 1, *and*
(b) *Whenever $\mu : X \longrightarrow G$ is a map converging to* 1 *of X into a pro-$\mathcal{C}$ group G and $\mu(X)$ is a set of generators of G, then there exists a unique homomorphism $\bar{\mu} : F_{\mathcal{C}}(X) \longrightarrow G$ that extends μ.*

---

* Some authors refer to what we call the free pro-$\mathcal{C}$ group on the set X converging to 1 as a *restricted free pro-$\mathcal{C}$ group on the set X*, and they denote it by $F^r_{\mathcal{C}}(X)$.

We shall refer to the subset X of $F_{\mathcal{C}}(X)$ as a *basis converging to* 1 or simply as a *basis* of the free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(X)$. As we have indicated before, we shall prove later (see Proposition 3.5.12) that every free pro-$\mathcal{C}$ group on a topological space (or a pointed topological space) is in fact also a free pro-$\mathcal{C}$ group on a set converging to 1. So from now on in this book the word "basis" for a free pro-$\mathcal{C}$ group will be used only in the sense of being a basis converging to 1 of a free pro-$\mathcal{C}$ group. Any other type of basis will be qualified, for example "topological basis".

Lemma 3.3.5

(a) *Let $F = F_{\mathcal{C}}(X)$ be a free pro-$\mathcal{C}$ group on a set X converging to* 1. *If F is also free pro-$\mathcal{C}$ on a set Y converging to* 1, *then the bases X and Y have the same cardinality.*
(b) *Let F be a free pro-$\mathcal{C}$ group on a finite set $X = \{x_1, \dots, x_n\}$. Then, any set of generators $\{y_1, \dots, y_n\}$ of F with n elements is a basis of F.*

Proof. (a) Say X and Y are two bases of F. If both X and Y are infinite, the result follows from Proposition 2.6.2. Say that $X = \{x_1, \dots, x_n\}$ is finite and assume that $|Y| > n$. We show that this is not possible. Indeed, choose a subset $X' = \{x'_1, \dots, x'_n\}$ of Y, and define a map $\mu : Y \longrightarrow F$ by $\mu(x'_i) = x_i$ $(i = 1, \dots, n)$ and $\mu(y) = 1$ if $y \in Y - X'$. Since μ converges to 1, it extends to a continuous epimorphism $\bar{\mu} : F \longrightarrow F$; then, by Proposition 2.5.2, $\bar{\mu}$ is an isomorphism, a contradiction.

(b) Consider the continuous epimorphism $\psi : F \longrightarrow F$ determined by $\psi(x_i) = y_i$ $(i = 1, \dots, n)$. Then ψ is an isomorphism by Proposition 2.5.2. □

If $F = F_{\mathcal{C}}(X)$ is a free pro-$\mathcal{C}$ group on the set X converging to 1, the *rank* of F is defined to be the cardinality of X. It is denoted by $\mathrm{rank}(F)$. Given a cardinal number $\mathfrak{m}$, we denote by $F_{\mathcal{C}}(\mathfrak{m})$ or $F(\mathfrak{m})$ a free pro-$\mathcal{C}$ group (on a set converging to 1) of rank $\mathfrak{m}$.

We state the next result for easy reference. It follows immediately from the definition of rank given above and the construction of free pro-$\mathcal{C}$ groups in the proof of Proposition 3.3.2.

Proposition 3.3.6 *Let Φ be an abstract free group on a finite basis X. Then the pro-$\mathcal{C}$ completion $\Phi_{\hat{\mathcal{C}}}$ of Φ is a free pro-$\mathcal{C}$ group on X. In particular,* $\mathrm{rank}(\Phi) = \mathrm{rank}(\Phi_{\hat{\mathcal{C}}})$.

Exercise 3.3.7 Show that if $F = F_{\mathcal{C}}(X, *)$ is the free pro-$\mathcal{C}$ group on the pointed profinite space $(X, *)$ and F is finitely generated, then $|X|$ is finite, and F is the free pro-$\mathcal{C}$ group of rank $|X| - 1$.

Example 3.3.8

(a) The free profinite group of rank 1 is $\widehat{\mathbf{Z}}$. Observe that $\widehat{\mathbf{Z}}$ is the free prosolvable (or proabelian, pronilpotent, etc.) group of rank 1, as well.
(b) If p is a prime number, then $\mathbf{Z}_p$ is the free pro-p group of rank 1.

(c) Let X be any set. Then the free proabelian group on the set X converging to 1 is the direct product $\prod_X \widehat{\mathbf{Z}}$ of copies of $\widehat{\mathbf{Z}}$ indexed by X. The canonical map $\iota : X \longrightarrow \prod_X \widehat{\mathbf{Z}}$ sends $x \in X$ to the tuple $(a_y) \in \prod_X \widehat{\mathbf{Z}}$ such that $a_y = 0$ for $y \neq x$ and $a_x = 1$. One sees this easily. Indeed, if $\varphi : X \longrightarrow A$ is a map converging to 1 onto a finite abelian group A, let Y be a finite subset of X such that $\varphi(x) = 0$ for all $x \in X - Y$. Then $\prod_X \widehat{\mathbf{Z}} = (\bigoplus_Y \widehat{\mathbf{Z}}) \oplus (\prod_{X-Y} \widehat{\mathbf{Z}})$. Define the corresponding continuous homomorphism $\bar{\varphi} : \prod_X \widehat{\mathbf{Z}} \longrightarrow A$ to be 0 on $\prod_{X-Y} \widehat{\mathbf{Z}}$, and the natural extension homomorphism on the finite indexed direct sum $\bigoplus_Y \widehat{\mathbf{Z}}$.

(d) Similarly, let $\mathcal{C}$ be the class of all finite abelian groups of exponent p, where p is a prime. Then the free pro-$\mathcal{C}$ group on the set X converging to 1 is the direct product $\prod_X \mathbf{Z}/p\mathbf{Z}$ of copies of $\mathbf{Z}/p\mathbf{Z}$ indexed by X.

(e) (cf. Douady, Harbater [1964, 1995]; see also Ribes [1970], p. 70; van den Dries and Ribenboim [1986]) Let F be an algebraically closed field, and denote by $\overline{F(t)}$ the algebraic closure of the field $F(t)$, where t is an indeterminate. Then the Galois group $G_{\overline{F(t)}/F(t)}$ is a free profinite group on a set converging to 1 of rank $|F|$.

Proposition 3.3.9 *Let $(X, *)$ be a pointed profinite space.*

(a) *Assume that*

$$(X, *) = \varprojlim_{i \in I} (X_i, *),$$

where $\{(X_i, *), \psi_{ij}\}$ is an inverse system of pointed profinite spaces. Then

$$F = F_{\mathcal{C}}(X, *) = \varprojlim_{i \in I} F_{\mathcal{C}}(X_i, *).$$

(b)

$$F = F_{\mathcal{C}}(X, *) = \varprojlim_{i \in I} F_{\mathcal{C}}(Y_i),$$

where each Y_i is a finite space, and $(X, *) = \varprojlim_{i \in I} (Y_i \,\dot\cup\, \{*\}, *)$.

Proof. (a) The inverse system $\{(X_i, *), \psi_{ij}\}$ determines an inverse system of free groups $\{F_{\mathcal{C}}(X_i, *), \bar{\psi}_{ij}\}$. For each $i \in I$, denote by $\psi_i : (X, *) \longrightarrow (X_i, *)$ the canonical projection. Correspondingly, one has continuous homomorphisms of groups $\bar{\psi}_i : F_{\mathcal{C}}(X, *) \longrightarrow F_{\mathcal{C}}(X_i, *)$, which are compatible with the mappings $\bar{\psi}_{ij}$. These homomorphisms induce then a continuous homomorphism of groups

$$\psi : F_{\mathcal{C}}(X, *) \longrightarrow G = \varprojlim_{i \in I} F_{\mathcal{C}}(X_i, *).$$

Denote by ι' the restriction of ψ to X; note that ι' is a mapping of pointed spaces. We claim that $\iota'(X)$ generates G as a topological group. To see this consider an epimorphism $\rho : G \longrightarrow H$ where $H \in \mathcal{C}$. It suffices to show that $\rho\iota'(X)$ generates H. By Lemma 1.1.16, ρ factors through $F(X_{i_0})$, for some $i_0 \in I$, i.e., there exists an epimorphism $\rho' : F(X_{i_0}) \longrightarrow H$ such that $\rho = \bar{\psi}_{i_0}\rho'$. Put $Y = \rho'(X_{i_0})$. Since H is finite, i_0 can be chosen so that $Y = \rho'\bar{\psi}_{ii_0}(X_{i_0})$, whenever $i \in I$, $i \geq i_0$. Since

$$(X, *) = \varprojlim_{i \geq i_0} (X_i, *),$$

we deduce that $Y = \rho\iota'(X)$, as needed.

To prove that

$$(\varprojlim_{i \in I} F_{\mathcal{C}}(X_i, *), \iota')$$

is the free pro-$\mathcal{C}$ group on the pointed space $(X, *)$, it remains to show that this pair satisfies the required universal property. Let $\mu : X \longrightarrow H$ be a continuous mapping with $\mu(*) = 1$, where $H \in \mathcal{C}$ and $\mu(X)$ generates H. Since H is finite, there exists some $j \in I$ and a continuous mapping of pointed spaces $\mu_j : (X_j, *) \longrightarrow (H, 1)$ such that $\mu_j\psi_j = \mu$ (see Lemma 1.1.16). Now, μ_j extends to a homomorphism $\bar{\mu}_j : F_{\mathcal{C}}(X_j, *) \longrightarrow H$. Define

$$\bar{\mu} : \varprojlim_{i \in I} F_{\mathcal{C}}(X_i, *) \longrightarrow H$$

by $\bar{\mu} = \bar{\mu}_j\bar{\psi}_j$. Then clearly $\bar{\mu}\iota' = \mu$.

(b) By definition we can express $(X, *)$ as an inverse limit of finite pointed spaces

$$(X, *) = \varprojlim_{i \in I} (X_i, *).$$

Put $Y_i = X_i - \{*\}$. Clearly $F_{\mathcal{C}}(X_i, *) = F_{\mathcal{C}}(Y_i)$. The result follows then from part (a). □

Let X be a set and let $\{X_i \mid i \in I\}$ be the collection of all finite subsets of X. Make I into a poset by defining $i \preceq j$ if $X_i \subseteq X_j$. If $i \preceq j$ define $\varphi_{ji} : F_{\mathcal{C}}(X_j) \longrightarrow F_{\mathcal{C}}(X_i)$ as the epimorphism that carries x to x, if $x \in X_i$, and x to 1, if $x \in X_j - X_i$ ($x \in X$). Observe that $\varprojlim (X_i \cup \{1\}, 1)$ is the one-point compactification of X. Then from Proposition 3.3.9 we deduce

Corollary 3.3.10 *Let X be a set and let $\{X_i \mid i \in I\}$ be the collection of all finite subsets X_i of X. Then*

(a) *For each $i \in I$, $F_{\mathcal{C}}(X_i)$ is a closed subgroup of the free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(X)$ on the set X converging to* 1;

(b)

$$F_{\mathcal{C}}(X) = \varprojlim_{i \in I} F_{\mathcal{C}}(X_i),$$

where the canonical homomorphism

$$\varphi_i : F_{\mathcal{C}}(X) \longrightarrow F_{\mathcal{C}}(X_i)$$

is the extension of the mapping $X \longrightarrow F_{\mathcal{C}}(X_i)$ *that sends* x *to* x *for* $x \in X_i$, *and* x *to* 1 *for* $x \in X - X_i$ $(x \in X)$.

This corollary can be improved in such a way that for a given open subgroup H of $F_{\mathcal{C}}(X)$, the mappings φ_i preserve the index of H. Before we make this precise, we need the following

Lemma 3.3.11 *Let* $Y \subseteq X$ *be sets and let* $F_{\mathcal{C}}(X)$ *and* $F_{\mathcal{C}}(Y)$ *be the corresponding free pro-*$\mathcal{C}$ *groups on the sets* X *and* Y *converging to* 1, *respectively. Consider the epimorphism*

$$\varphi : F_{\mathcal{C}}(X) \longrightarrow F_{\mathcal{C}}(Y)$$

defined by

$$\varphi(x) = \begin{cases} x & \text{if } x \in Y, \\ 1 & \text{if } x \notin Y. \end{cases}$$

Then the following is a split exact sequence

$$1 \longrightarrow N \longrightarrow F_{\mathcal{C}}(X) \xrightarrow{\varphi} F_{\mathcal{C}}(Y) \longrightarrow 1,$$

where N *is the smallest closed normal subgroup generated by* $X - Y$. (*This means that there is a continuous section of* φ *which is a homomorphism, i.e., that* $F_{\mathcal{C}}(X)$ *is a semidirect product of* N *by a closed subgroup isomorphic to* $F_{\mathcal{C}}(Y)$.)

Proof. Define a continuous homomorphism $\sigma : F_{\mathcal{C}}(Y) \longrightarrow F_{\mathcal{C}}(X)$ by $\sigma(y) = y$, for all $y \in Y$. Then σ is a section of φ. Let $K = \mathrm{Ker}(\varphi)$. After identifying $F_{\mathcal{C}}(Y)$ with $\sigma(F_{\mathcal{C}}(Y))$, we have $F = NF_{\mathcal{C}}(Y) = KF_{\mathcal{C}}(Y)$. Since

$$N \cap F_{\mathcal{C}}(Y) = K \cap F_{\mathcal{C}}(Y) = 1 \quad \text{and} \quad N \le K,$$

it follows that $N = K$. □

Proposition 3.3.12 *Let* $F_{\mathcal{C}}(X)$ *be a free pro-*$\mathcal{C}$ *group on a set* X *converging to* 1 *and* $H \le_o F_{\mathcal{C}}(X)$. *Then there is a collection* $\{X_j \mid j \in J\}$ *of finite subsets of* X *such that*

(a) $\{F_{\mathcal{C}}(X_j), \varphi_{jk}, J\}$ *is an inverse system of free pro-*$\mathcal{C}$ *groups, where if* $X_j \supseteq X_k$, *the epimorphism* $\varphi_{jk} : F_{\mathcal{C}}(X_j) \longrightarrow F_{\mathcal{C}}(X_k)$ *is defined by*

$$\varphi_{jk}(x) = \begin{cases} x & \text{if } x \in X_k, \\ 1 & \text{if } x \in X_j - X_k; \end{cases}$$

(b)

$$F_{\mathcal{C}}(X) = \varprojlim_{j \in J} F_{\mathcal{C}}(X_j); \quad \text{and}$$

(c)

$$[F_{\mathcal{C}}(X_j) : \varphi_j(H)] = [F_{\mathcal{C}}(X) : H],$$

for every $j \in J$, where $\varphi_j : F_{\mathcal{C}}(X) \longrightarrow F_{\mathcal{C}}(X_j)$ is the canonical projection.

Proof. Put $F = F_{\mathcal{C}}(X)$. Let $H_F = \bigcap_{f \in F} f^{-1}Hf$ (the core of H in F). Then H_F is an open normal subgroup of F contained in H. Let $\{X_i \mid i \in I\}$ be the collection of all finite subsets of X. Make I into a directed poset by defining $i \preceq j$ if $X_i \subseteq X_j$ $(i, j \in I)$. Set

$$J = \{i \in I \mid X - X_i \subseteq H_F\}.$$

Clearly J is a cofinal subset of the poset I since $X - (X \cap H_F)$ is a finite set. Statement (a) is clear. Part (b) follows from Corollary 3.3.10 and Lemma 1.1.9. To prove (c), just observe that according to Lemma 3.3.11, $\mathrm{Ker}(\varphi_j) \leq H_F \leq H$. □

Proposition 3.3.13 *Let $F = F_{\mathcal{C}}(X, *)$ be the free pro-$\mathcal{C}$ group on a pointed profinite space $(X, *)$. Assume that every abstract free group of finite rank is residually $\mathcal{C}$. Then the abstract subgroup of F generated by X is a free abstract group on $X - \{*\}$.*

Proof. Let $D = D(X - \{*\})$ be the abstract free group on $X - \{*\}$, and denote by $\psi : D \longrightarrow F$ the natural homomorphism induced by the canonical injection $\iota : (X, *) \longrightarrow F$. We must show that ψ is a monomorphism. Let $w = x_1^{\epsilon_1} \cdots x_r^{\epsilon_r}$ be a reduced word on $X - \{*\}$, i.e., $x_i \in X - \{*\}, \epsilon_i = \pm 1, \epsilon_i \neq -\epsilon_{i+1}$ if $x_i = x_{i+1}$ $(i = 1, \ldots, r)$. Choose an open equivalence relation R of X such that if $x, y \in \{x_1, \ldots, x_r\}$ and $x \neq y$, then $xR \neq yR$ in X/R. Then the corresponding element $w' = x_1^{\epsilon_1}R \cdots x_r^{\epsilon_r}R$ of the abstract free group $D = D(X/R - \{*R\})$ is also in reduced form. Hence if $w \neq 1$, then $w' \neq 1$. So, from the commutativity of the diagram

$$\begin{array}{ccc} D(X - \{*\}) & \xrightarrow{\psi} & F_{\mathcal{C}}(X, *) \\ \downarrow & & \downarrow \\ D(X/R - \{*R\}) & \xrightarrow[\psi_R]{} & F_{\mathcal{C}}(X/R, *R) \end{array}$$

we deduce that we may assume that X is a finite space. Now, from the construction of F (see the proof of Proposition 3.3.2), we get that

$$\mathrm{Ker}(\psi) = \bigcap \{N \triangleleft D \mid D/N \in \mathcal{C}\},$$

since X is finite. Therefore $\mathrm{Ker}(\psi) = 1$, for D is residually $\mathcal{C}$. □

Corollary 3.3.14 *Let $F = F_{\mathcal{C}}(X)$ be a free pro-$\mathcal{C}$ group on a set X converging to 1. Assume that every abstract free group of finite rank is residually $\mathcal{C}$. Then the abstract subgroup of F generated by X is a free abstract group on X.*

We remark that the hypotheses in Proposition 3.3.13 and Corollary 3.3.14 are valid for many classes $\mathcal{C}$ of interest, as we show in the following proposition.

Proposition 3.3.15 *Let Φ be an abstract free group and let S be a finite simple group such that the rank of Φ is at least $d(S)$.*[†] *Assume that $\mathcal{C}$ is a formation that contains all S-groups. Then Φ is residually $\mathcal{C}$. In particular, if $\mathcal{C}$ is a nontrivial NE-formation of finite groups, then every abstract free group is residually $\mathcal{C}$.*

Proof. The last statement is a consequence of the first part of the lemma, since a nontrivial NE-formation of finite groups contains all S-groups for some finite simple group S. To prove the first part, it suffices to show that Φ is residually a finite S-group. We may assume that Φ has finite rank.

Case 1: $S = C_p$ for some prime p.

We use the well-known fact that the matrices

$$\begin{bmatrix} 1 & 0 \\ p & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & p \\ 0 & 1 \end{bmatrix}$$

generate an abstract free subgroup of $\mathrm{SL}_2(\mathbf{Z})$ of rank 2. Let $\Gamma(p^i)$ be the kernel of the natural map $\mathrm{SL}_2(\mathbf{Z}) \longrightarrow \mathrm{SL}_2(\mathbf{Z}/p^i\mathbf{Z})$. It follows that Φ can be embedded as a subgroup of $\Gamma(p)$. Hence, it suffices to prove that $\Gamma(p)$ is residually a finite p-group. Remark that the elements of $\Gamma(p^i)$ are those elements in $\mathrm{SL}_2(\mathbf{Z})$ the form $I + p^i A$, where I is the identity matrix and A is a 2×2 matrix over $\mathbf{Z}$. Clearly $\bigcap_{i=1}^{\infty} \Gamma(p^i) = \{I\}$ and each quotient group $\mathrm{SL}_2(\mathbf{Z})/\Gamma(p^i)$ is finite. Next, observe that for $I + p^i A \in \Gamma(p^i)$, one has

$$(I + p^i A)^p = \sum_{j=0}^{p} \binom{p}{j} (p^k A)^j \equiv I \mod \Gamma(p^{i+1}).$$

One deduces that $\Gamma(p)/\Gamma(p^k)$ is a finite p-group for all $k = 2, 3, \ldots$.

Case 2: S is a nonabelian simple group.

Set $M^0 = \Phi$, and in general, $M^{n+1} = M_S(M^n)$, the intersection of all normal subgroups N of M^n with $M^n/N \cong S$. Clearly each M^n is a proper characteristic subgroup of Φ of rank at least $d(S)$, and M^n/M^{n+1} is a finite S-group. By a result of Levi (cf. Lyndon and Schupp [1977], Proposition I.3.3), $\bigcap_{n=0}^{\infty} M^n = 1$. Thus Φ is residually a finite S-group. □

Theorem 3.3.16 *Let G be a pro-$\mathcal{C}$ group. Then there exists a free pro-$\mathcal{C}$ group F on a set converging to 1 and a continuous epimorphism $F \longrightarrow G$. Furthermore, if G is generated by a finite set with n elements, then F can be chosen to have rank n; while if G is not finitely generated, then F can be chosen to have rank equal to $\omega_0(G)$, the smallest cardinal of a fundamental system of neighborhoods of 1 in G.*

[†] By the classification theorem of finite simple groups $d(S) = 2$ for a nonabelian finite simple group S.

Proof. By Proposition 2.4.4, G admits a set of generators X converging to 1. Consider the free pro-$\mathcal{C}$ group $F = F_{\mathcal{C}}(\tilde{X})$ on the set $\tilde{X}$ converging to 1, where $\tilde{X}$ is a set with the same cardinality as X. Say that $\varphi : \tilde{X} \longrightarrow X$ is a bijection. Then the composite

$$\tilde{X} \xrightarrow{\varphi} X \hookrightarrow G$$

is a mapping converging to 1, and so it extends to an epimorphism

$$\bar{\varphi} : F(\tilde{X}) \longrightarrow G.$$

If X is infinite, then $|X| = \omega_0(G)$ by Proposition 2.6.1, and therefore, $\mathrm{rank}(F(\tilde{X})) = \omega_0(G)$. □

3.4 Maximal Pro-$\mathcal{C}$ Quotient Groups

In this section we establish a relationship between free groups over the same space when the formation $\mathcal{C}$ changes. First we define a subgroup of a profinite group associated with the class $\mathcal{C}$.

Let $\mathcal{C}$ be a formation of finite groups. For a profinite group G, define

$$R_{\mathcal{C}}(G) = \bigcap\{N \mid N \triangleleft_o G, G/N \in \mathcal{C}\}.$$

Remark that $R_{\mathcal{C}}(G)$ is a characteristic subgroup of G. If p is a fixed prime number and $\mathcal{C}$ consists of all finite p-groups, we write $R_p(G)$ rather than $R_{\mathcal{C}}(G)$. The subgroups $R_{\mathcal{C}}(G)$ play a role similar to verbal subgroups in the theory of abstract groups.

Lemma 3.4.1 *Let G and H be profinite groups. Let $\mathcal{C}$ be a formation of finite groups.*

(a) *$G/R_{\mathcal{C}}(G)$ is the largest pro-$\mathcal{C}$ quotient group of G, i.e., if $K \triangleleft_c G$ and G/K is a pro-$\mathcal{C}$ group, then $K \geq R_{\mathcal{C}}(G)$.*
(b) *If $\varphi : G \longrightarrow H$ is a continuous epimorphism, then $\varphi(R_{\mathcal{C}}(G)) = R_{\mathcal{C}}(H)$.*
(c) *Assume that $\mathcal{C}$ is, in addition, closed under taking subgroups, i.e., $\mathcal{C}$ a variety of finite groups. Then, if $\varphi : G \longrightarrow H$ is a continuous homomorphism, then $\varphi(R_{\mathcal{C}}(G)) \leq R_{\mathcal{C}}(H)$.*
(d) *Suppose that the formation $\mathcal{C}$ is closed under taking normal subgroups and extensions (i.e., $\mathcal{C}$ is an NE-formation). Then, if $R_{\mathcal{C}}(G) \leq K \triangleleft_c G$, one has $R_{\mathcal{C}}(G) = R_{\mathcal{C}}(K)$.*
(e) *Suppose that $\mathcal{C}$ is an NE-formation of finite groups. If $L \triangleleft_c R_{\mathcal{C}}(G)$ and $R_{\mathcal{C}}(G)/L$ is a pro-$\mathcal{C}$ group, then $L = R_{\mathcal{C}}(G)$.*

Proof. Part (a) is plain.

(b) Since $\mathcal{C}$ is a formation, the collection of all closed normal subgroups N of G such that G/N is a pro-$\mathcal{C}$ group is filtered from below. Hence part (b) follows from Proposition 2.1.4(b).

(c) Put $B = \varphi(G)$. Note that

$$B/B \cap R_{\mathcal{C}}(H) \cong BR_{\mathcal{C}}(H)/R_{\mathcal{C}}(H) \hookrightarrow H/R_{\mathcal{C}}(H).$$

Since $\mathcal{C}$ is a variety, we have that $B/B \cap R_{\mathcal{C}}(H)$ is a pro-$\mathcal{C}$ group. Hence, $R_{\mathcal{C}}(B) \leq B \cap R_{\mathcal{C}}(H)$. By part (b), $R_{\mathcal{C}}(G) = R_{\mathcal{C}}(B)$. Thus, $R_{\mathcal{C}}(G) \leq R_{\mathcal{C}}(H)$.

(d) Put $R = R_{\mathcal{C}}(G)$. Observe that $K/R \triangleleft G/R$. Hence K/R is a pro-$\mathcal{C}$ group. Therefore, $R_{\mathcal{C}}(K) \leq R$. Since $R_{\mathcal{C}}(K)$ is a characteristic subgroup of K and K is normal in G, it follows that $R_{\mathcal{C}}(K) \triangleleft G$. Since $\mathcal{C}$ is extension closed, $G/R_{\mathcal{C}}(K)$ is a pro-$\mathcal{C}$ group. Thus $R_{\mathcal{C}}(K) = R$.

(e) This is clear from part (d) since $R_{\mathcal{C}}(R_{\mathcal{C}}(G)) = R_{\mathcal{C}}(G)$. □

Proposition 3.4.2 *Let $\mathcal{C}'$ and $\mathcal{C}$ be formations of finite groups with $\mathcal{C}' \subseteq \mathcal{C}$. Let $F = F_{\mathcal{C}}(X,*)$ be a free pro-$\mathcal{C}$ group on the pointed space $(X,*)$. Then*

$$F_{\mathcal{C}}(X,*)/R_{\mathcal{C}'}(F_{\mathcal{C}}(X,*)) \cong F_{\mathcal{C}'}(X,*).$$

Proof. Let $\iota : (X,*) \longrightarrow F_{\mathcal{C}}(X,*)$ be the canonical embedding and

$$\mu : F_{\mathcal{C}}(X,*) \longrightarrow F_{\mathcal{C}}(X,*)/R_{\mathcal{C}'}(F_{\mathcal{C}}(X,*))$$

the natural epimorphism. Then one easily checks (using Lemma 3.4.1) that the pair

$$(F_{\mathcal{C}}(X,*)/R_{\mathcal{C}'}(F_{\mathcal{C}}(X,*)), \mu\iota),$$

where

$$\mu\iota : (X,*) \longrightarrow F_{\mathcal{C}}(X,*)/R_{\mathcal{C}'}(F_{\mathcal{C}}(X,*)),$$

satisfies the universal property of a free pro-$\mathcal{C}'$ group on the pointed space $(X,*)$. □

We say that a variety of finite groups $\mathcal{C}$ is closed under 'extensions with abelian kernel' if whenever

$$1 \longrightarrow A \longrightarrow G \longrightarrow H \longrightarrow 1$$

is an exact sequence of finite groups such that $A, H \in \mathcal{C}$ and A is abelian, then $G \in \mathcal{C}$.

Lemma 3.4.3 *Let $\mathcal{C}$ be a variety of finite groups and let $\mathcal{C}_e$ be the smallest extension closed variety of finite groups containing $\mathcal{C}$. For a given pointed profinite space $(X,*)$, denote by K_X the kernel of the natural epimorphism*

$$\varphi_X : F_{\mathcal{C}_e}(X,*) \longrightarrow F_{\mathcal{C}}(X,*).$$

Then, K_X is perfect (i.e., $K_X = \overline{[K_X, K_X]}$) for every profinite space X if and only if $\mathcal{C}$ is closed under extensions with abelian kernel.

Proof. Express $(X,*) = \varprojlim (X_i,*)$ as a surjective inverse limit of pointed finite discrete spaces. Then $K_X = \varprojlim K_{X_i}$. Hence one may assume that X is finite and discrete (non pointed).

Suppose that $\mathcal{C}$ is closed under extensions with abelian kernel. Choose a finite discrete space X. We have to show that K_X is perfect. Put $K = K_X$ and $\varphi = \varphi_X$. Then, one has a short exact sequence

$$1 \longrightarrow K/\overline{[K,K]} \longrightarrow F_{\mathcal{C}_e}(X)/\overline{[K,K]} \longrightarrow F_{\mathcal{C}}(X) \longrightarrow 1.$$

From the definition of $\mathcal{C}_e$ and the assumption on $\mathcal{C}$, one sees that $\mathcal{C}$ and $\mathcal{C}_e$ contain the same abelian groups. Hence, $K/\overline{[K,K]}$ is a pro-$\mathcal{C}$ group. Again, from our assumption on $\mathcal{C}$, it follows that $F_{\mathcal{C}_e}(X)/\overline{[K,K]}$ is a pro-$\mathcal{C}$ group. Therefore, there exists a continuous epimorphism

$$\mu : F_{\mathcal{C}}(X) \longrightarrow F_{\mathcal{C}_e}(X)/\overline{[K,K]}.$$

By Proposition 2.5.2, the epimorphism

$$F_{\mathcal{C}}(X) \xrightarrow{\mu} F_{\mathcal{C}_e}(X)/\overline{[K,K]} \longrightarrow F_{\mathcal{C}_e}(X)/K \xrightarrow{\cong} F_{\mathcal{C}}(X)$$

is an isomorphim. Thus, $K = \overline{[K,K]}$.

Conversely, suppose that $\mathcal{C}$ is not closed under extensions with abelian kernel. Consider a short exact sequence

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\alpha} H \longrightarrow 1,$$

where $A, H \in \mathcal{C}$, A is finite abelian and $G \notin \mathcal{C}$. We shall show that K_X is not perfect for a certain finite discrete space X. Choose X to be such that $|X| = d(G)$. Choose a continuous epimorphism $\beta : F_{\mathcal{C}}(X) \longrightarrow H$. By a property of free pro-$\mathcal{C}$ groups that we prove in the next section (see Theorem 3.5.8), one has a continuous epimorphism $\psi : F_{\mathcal{C}_e}(X) \longrightarrow G$ such that $\alpha\psi = \beta\varphi_X$. This implies that $\psi(K_X)$ is contained in A. We claim that K_X is not perfect. To see this, it suffices to show that $\psi(K_X) \neq 1$, since A is abelian. Now, if we had $\psi(K_X) = 1$, then ψ would factor through $F_{\mathcal{C}}(X)$. Thus, G would be in $\mathcal{C}$, a contradiction. □

3.5 Characterization of Free Pro-$\mathcal{C}$ Groups

Definition 3.5.1 *Let G be a profinite group. Let $\mathcal{E}$ be a nonempty class of continuous epimorphisms*

$$\alpha : A \longrightarrow B \tag{4}$$

of profinite groups. Denote by $\mathcal{E}_f$ the subclass of $\mathcal{E}$ consisting of those epimorphisms (4) such that $K = \mathrm{Ker}(\alpha)$ is a finite minimal normal subgroup of A.

(a) *An $\mathcal{E}$-embedding problem for G is a diagram*

$$\begin{array}{ccc} & & G \\ & & \downarrow{\scriptstyle\varphi} \\ A & \xrightarrow{\alpha} & B \end{array}$$

or, written more explicitly,

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array} \tag{5}$$

with exact row, where $\alpha \in \mathcal{E}$ and φ is a continuous epimorphism of profinite groups. We say that the $\mathcal{E}$-embedding problem (5) *is 'solvable' or that it 'has a solution' if there exists a continuous epimorphism*

$$\bar{\varphi} : G \longrightarrow A$$

such that $\alpha\bar{\varphi} = \varphi$. The above $\mathcal{E}$-embedding problem is said to be 'weakly solvable' or to have a 'weak solution' if there is a continuous homomorphism

$$\bar{\varphi} : G \longrightarrow A$$

such that $\alpha\bar{\varphi} = \varphi$.

(b) *The kernel of the $\mathcal{E}$-embedding problem* (5) *is the group $K = \mathrm{Ker}(\alpha)$. We say that the $\mathcal{E}$-embedding problem* (5) *has 'finite minimal normal kernel' if α is in $\mathcal{E}_f$.*

(c) *The nonempty class $\mathcal{E}$ of extensions is 'admissible' if whenever*

$$\alpha : A \longrightarrow B$$

is in $\mathcal{E}$, so are the corresponding epimorphisms

$$A \longrightarrow A/N \quad \text{and} \quad A/N \longrightarrow B,$$

for any closed normal subgroup N of A contained in $\mathrm{Ker}(\alpha)$.

(d) *An infinite profinite group G is said to have the 'strong lifting property' over a class of epimorphisms $\mathcal{E}$ if every $\mathcal{E}$-embedding problem* (5) *with $w_0(B) < w_0(G)$ and $w_0(A) \le w_0(G)$ is solvable.*

Remark 3.5.2 The term 'embedding problem' has its origins in Galois theory. Denote by $\bar{F}$ an algebraic separable closure of a given field F. The Galois group $G_{\bar{F}/F}$ of the extension $\bar{F}/F$ is called the *absolute Galois group of F*. Let K/F be a Galois extension of fields and let $\alpha : H' \longrightarrow H$ be a continuous epimorphism of profinite groups. Assume that $H = G_{K/F}$, the Galois group of K/F. Then there is an epimorphism

$$\varphi: G_{\bar{F}/F} \longrightarrow H = G_{K/F}$$

defined by restricting the automorphisms in $G_{\bar{F}/F}$ to K. One question that arises often in Galois theory is the following: does there exist a subfield K' of $\bar{F}$ containing K in such a way that $H' = G_{K'/F}$ and the natural epimorphism $G_{K'/F} \longrightarrow G_{K/F}$ is precisely α? Observe that this question is equivalent to asking whether there is a solution of the following embedding problem:

$$\begin{array}{ccc} & & G_{\bar{F}/F} \\ & & \downarrow{\scriptstyle\varphi} \\ H' & \xrightarrow{\alpha} & H. \end{array}$$

This question is sometimes referred to as the 'inverse problem of Galois theory'.

Let $\mathbf{Q}$, the field of rational numbers. A well-known question in algebraic number theory is whether every finite group appears as a Galois group of a Galois extension of $\mathbf{Q}$. Or, equivalently,

Open Question 3.5.3 *Is every finite group a continuous homomorphic image of the absolute Galois group $G_{\bar{\mathbf{Q}}/\mathbf{Q}}$ of the field $\mathbf{Q}$ of rational numbers?*

For some additional information on this question see Section 3.7.

Let $\mathcal{C}$ be a formation. Observe that if $\mathcal{E}$ is an admissible class, then so is $\mathcal{E}_f$. The class of all continuous epimorphisms of pro-$\mathcal{C}$ groups is an example of admissible class that we shall use frequently.

Lemma 3.5.4 *Let $\mathcal{E}$ be an admissible class of continuous epimorphisms of profinite groups and let G be a profinite group. The following conditions are equivalent.*

(a) *G has the strong lifting property over $\mathcal{E}$;*
(b) *G has the strong lifting property over $\mathcal{E}_f$.*

Proof. The implication (a) $\Rightarrow$ (b) is obvious.

(b) $\Rightarrow$ (a): Suppose G has the strong lifting property over $\mathcal{E}_f$ and let (5) be a $\mathcal{E}$-embedding problem with $w_0(B) < w_0(G)$ and $w_0(A) \leq w_0(G)$. By Corollary 2.6.5, there exist an ordinal number μ and a chain of closed subgroups of K (see diagram (5))

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

such that

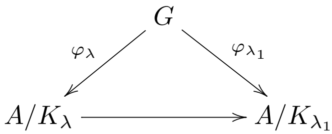
(i) each K_λ is a normal subgroup of A with $K_\lambda/K_{\lambda+1}$ finite; moreover, $K_{\lambda+1}$ is maximal in K_λ with respect to these properties;
(ii) if λ is a limit ordinal, then $K_\lambda = \bigcap_{\nu<\lambda} K_\nu$; and

(iii) if $w_0(A) = w_0(G)$ (therefore K is an infinite group and $w_0(A/K) < w_0(A)$), then $w_0(A/K_\lambda) < w_0(A)$ whenever $\lambda < \mu$.

We must prove that there exists an epimorphism $\bar{\varphi} : G \longrightarrow A$ such that $\alpha\bar{\varphi} = \varphi$. To do this we show in fact that for each $\lambda \leq \mu$ there exists an epimorphism

$$\varphi_\lambda : G \longrightarrow A/K_\lambda$$

such that if $\lambda_1 \leq \lambda$ the diagram

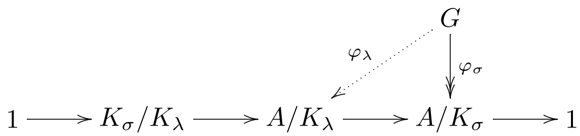


commutes, where the horizontal mapping is the natural epimorphism. Then we can take $\bar{\varphi} = \varphi_\mu$. To show the existence of φ_λ, we proceed by induction (transfinite, if K is infinite) on λ. Note that $A/K_0 = B$; so, put $\varphi_0 = \varphi$. Let $\lambda \leq \mu$ and assume that φ_ν has been defined for all $\nu < \lambda$ so that the above conditions are satisfied. If λ is a limit ordinal, observe that since $K_\lambda = \bigcap_{\nu<\lambda} K_\nu$, then

$$A/K_\lambda = \varprojlim_{\nu<\lambda} A/K_\nu;$$

in this case, define $\varphi_\lambda = \varprojlim_{\nu<\lambda}\varphi_\nu$.

If, on the other hand, $\lambda = \sigma + 1$, we define φ_λ to be a solution to the $\mathcal{E}_f$-embedding problem with finite minimal normal kernel



To see that such a solution exists, we have to verify that $w_0(A/K_\sigma) < w_0(G)$ and $w_0(A/K_\lambda) \leq w_0(G)$. If $w_0(A) < w_0(G)$, these inequalities are clear. On the other hand, if $w_0(A) = w_0(G)$, we have

$$w_0(A/K_\lambda) = w_0(A/K_\sigma) < w_0(A) = w_0(G),$$

since K_σ/K_λ is a finite group and since condition (iii) above holds.

It is clear that in either case φ_λ satisfies the required conditions. □

Next we consider equivalent conditions to weak solvability of embedding problems for some special types of admissible classes.

Lemma 3.5.5 *Let $\mathcal{C}$ and $\mathcal{C}'$ be varieties of finite groups. Let $\mathcal{E}$ be the class of all continuous epimorphisms* (4) *of pro-$\mathcal{C}$ groups such that* $\mathrm{Ker}(\alpha)$ *is pro-$\mathcal{C}'$, and let $\bar{\mathcal{E}}$ consist of those epimorphisms* (4) *in $\mathcal{E}$ for which* $\mathrm{Ker}(\alpha)$ *is finite. Let G be a profinite group. The following conditions are equivalent.*

(a) *Every $\mathcal{E}$-embedding problem* (5) *for G has a weak solution*;
(b) *Every $\bar{\mathcal{E}}$-embedding problem* (5) *for G has a weak solution*;
(c) *Every $\bar{\mathcal{E}}_a$-embedding problem* (5) *for G has a weak solution, where $\bar{\mathcal{E}}_a$ consists of those epimorphisms* (4) *in $\bar{\mathcal{E}}$ such that* $\mathrm{Ker}(\alpha)$ *is a finite abelian minimal normal subgroup of A.*

Proof. The implications (a) $\Rightarrow$ (b) $\Rightarrow$ (c) are clear.

(b) $\Rightarrow$ (a): Consider the embedding problem (5) with $\alpha \in \mathcal{E}$. Define a set $\mathcal{P}$ to consist of all pairs (K', η'), where K' is a closed normal subgroup of A contained in K, and $\eta' : G \longrightarrow A/K'$ is a continuous homomorphism such that the diagram

$$\begin{array}{ccc} & & G \\ & \swarrow^{\eta'} & \downarrow \varphi \\ A/K' & \longrightarrow & B \end{array}$$

commutes. The set $\mathcal{P}$ is nonempty since $(K, \varphi) \in \mathcal{P}$. Define $(K', \eta') \preceq (K'', \eta'')$ if $K' \geq K''$ and

$$\begin{array}{ccc} & & G \\ & \swarrow^{\eta'} & \downarrow \eta'' \\ A/K' & \longleftarrow & A/K'' \end{array}$$

commutes. Then $\mathcal{P}$ is an inductive poset. Indeed, if $\{(K'_i, \eta'_i)\}_i$ is a totally ordered subset of $\mathcal{P}$, put

$$K' = \bigcap_i K'_i \quad \text{and} \quad \eta' = \varprojlim_i \eta'_i;$$

then $(K', \eta') \in \mathcal{P}$ and $(K', \eta') \succeq (K'_i, \eta'_i)$ for all i.

Let $(\tilde{K}, \tilde{\eta})$ be a maximal element of $\mathcal{P}$. We shall show that $\tilde{K} = 1$. Suppose $\tilde{K} \neq 1$; then there exists an open normal subgroup L of $\tilde{K}$ which is normal in A, such that $L \neq \tilde{K}$ (if $\tilde{K} \neq 1$, it contains a proper open subgroup $\tilde{K} \cap U$ where U is open in A; then U contains an open normal subgroup V of A; put $L = K \cap V$).

Since $\tilde{K}/L$ is finite, it follows from (b) that there exists a continuous homomorphism

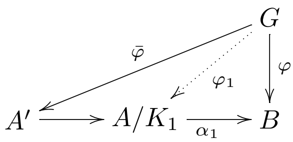
$$\psi : G \longrightarrow A/L$$

such that

$$\begin{array}{ccc} & & G \\ & \swarrow^{\psi} & \downarrow \tilde{\eta} \\ A/L & \longrightarrow & A/\tilde{K} \end{array}$$

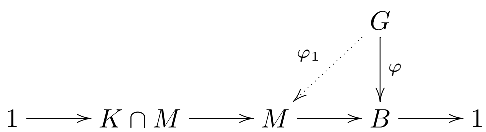
commutes. Hence, $(L, \psi) \in \mathcal{P}$ and $(L, \psi) \succ (\tilde{K}, \tilde{\eta})$, contradicting the maximality of $(\tilde{K}, \tilde{\eta})$. Thus $\tilde{K} = 1$.

(c) $\Rightarrow$ (b): We show in fact something stronger, namely that if (c) holds and we have a diagram (5) with $\alpha \in \bar{\mathcal{E}}$ and K finite, then there exists a continuous homomorphism $\bar{\varphi} : G \longrightarrow A$ making the diagram commutative. We prove this by induction on the order of K. We distinguish two cases depending on whether K is minimal normal in A or not. Suppose first the latter. Then there exists a normal subgroup K_1 of A such that $1 < K_1 < K$.



Let $\alpha_1 : A/K_1 \longrightarrow B$ be the epimorphism induced by α. Then, by induction, there exists a continuous homomorphism $\varphi_1 : G \longrightarrow A/K_1$ such that $\alpha_1\varphi_1 = \varphi$. Let $\beta : A \longrightarrow A/K_1$ be the canonical epimorphism, and set $A' = \beta^{-1}(\varphi_1(G))$. By induction again, there exists a continuous homomorphism $\bar{\varphi} : G \longrightarrow A'$ such that $\beta_{|A'}\bar{\varphi} = \varphi_1$. If we think of $\bar{\varphi}$ as a mapping $G \longrightarrow A$, then $\bar{\varphi}$ is the desired lifting.

Next assume that K is finite minimal normal in A. Consider the Frattini subgroup $\Phi(A)$ of A, and recall that $\Phi(A)$ is pronilpotent (see Corollary 2.8.4). By the minimality of K, either $K \leq \Phi(A)$ or $K \cap \Phi(A) = 1$. Assume first that $K \leq \Phi(A)$. Hence K is nilpotent, since it is finite. Observe that $[K, K] = 1$, for otherwise $[K, K] = K$, contradicting the nilpotency of K. Therefore, K is abelian. Then the existence of $\bar{\varphi}$ follows from (c). Suppose now that $K \cap \Phi(A) = 1$. Then there exists a maximal open subgroup M of A such that $K \not\leq M$. Hence $K \cap M < K$. Thus, by induction, there exists a continuous homomorphism $\varphi_1 : G \longrightarrow M$ making the diagram



commutative. Finally, define $\bar{\varphi} : G \longrightarrow A$ to be the composition

$$G \xrightarrow{\varphi_1} M \hookrightarrow A.$$

□

Having the strong lifting property over a suitable class of epimorphisms is a powerful property for a profinite group; in the following result it is used as a key tool to determine when two groups are isomorphic.

Proposition 3.5.6 *Let $\mathcal{E}$ be an admissible class of continuous epimorphisms of profinite groups and let G_1 and G_2 be infinite profinite groups with the* *strong lifting property over $\mathcal{E}$ and such that $w_0(G_1) = w_0(G_2) = \mathfrak{m}$. Assume that $N_i \lhd_c G_i$ such that $w_0(G_i/N_i) < \mathfrak{m}$ and that the epimorphisms*

$$G_i \longrightarrow G_i/N_i \longrightarrow 1$$

belong to $\mathcal{E}$ $(i = 1, 2)$. Then, any isomorphism $\varphi : G_1/N_1 \longrightarrow G_2/N_2$ lifts to an isomorphism $\bar{\varphi} : G_1 \longrightarrow G_2$ such that the diagram

$$\begin{array}{ccc} G_1 & \xrightarrow{\bar{\varphi}} & G_2 \\ \downarrow & & \downarrow \\ G_1/N_1 & \xrightarrow[\varphi]{} & G_2/N_2 \end{array}$$

commutes.

Proof. Let μ be the smallest ordinal with cardinality $\mathfrak{m}$. By Corollary 2.6.5, there exists a chain of closed normal subgroups of G_i $(i = 1, 2)$

$$N_i = N_{i,0} \geq N_{i,1} \geq \cdots \geq N_{i,\lambda} \geq \cdots \geq N_{i,\mu} = 1$$

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

(i) $N_{i,\lambda}/N_{i,\lambda+1}$ is finite for $\lambda \geq 0$;
(ii) if λ is a limit ordinal, then $N_{i,\lambda} = \bigcap_{\nu<\lambda} N_{i,\nu}$, and
(iii) $w_0(G_i/N_{i,\lambda}) < \mathfrak{m}$, for $\lambda < \mu$.

We shall use transfinite induction to construct chains of closed normal subgroups of G_i $(i = 1, 2)$

$$N_i = N'_{i,0} \geq N'_{i,1} \geq \cdots \geq N'_{i,\lambda} \geq \cdots \geq N'_{i,\mu} = 1$$

satisfying conditions analogous to (i), (ii), (iii), and in addition

(iv) $N'_{i,\lambda} \leq N_{i,\lambda}$ and $w_0(G_i/N'_{i,\lambda}) \leq w_0(G_i/N_{i,\lambda})$, for all λ $(i = 1, 2)$.

Note that conditions (iii) and (iv) imply that $w_0(G_i/N'_{i,\lambda}) < w_0(G_i)$ for all $\lambda < \mu$ $(i = 1, 2)$.

Furthermore, we construct isomorphisms

$$\varphi_\lambda : G_1/N'_{1,\lambda} \longrightarrow G_2/N'_{2,\lambda}$$

for each $\lambda \leq \mu$, in such a way that if $\lambda < \nu \leq \mu$, then the diagram

$$\begin{array}{ccc} G_1/N'_{1,\nu} & \xrightarrow{\varphi_\nu} & G_2/N'_{2,\nu} \\ \downarrow & & \downarrow \\ G_1/N'_{1,\lambda} & \xrightarrow[\varphi_\lambda]{} & G_2/N'_{2,\lambda} \end{array}$$

commutes. Set $N'_{i,0} = N_{i,0} = N_i$ $(i = 1, 2)$, and let $\varphi_0 : G_1/N'_{1,0} \longrightarrow G_2/N'_{2,0}$ be the given isomorphism φ. Let $\rho \leq \mu$ and assume we have constructed chains indexed by $\lambda < \rho$

$$N_i = N'_{i,0} \geq N'_{i,1} \geq \cdots \geq N'_{i,\lambda} \geq \cdots \quad (i = 1, 2)$$

as well as isomorphisms φ_λ $(\lambda < \rho)$, satisfying the above conditions. Next we indicate how to construct $N'_{i,\rho}$ $(i = 1, 2)$ and an isomorphism φ_ρ such that the above conditions still hold. If ρ is a limit ordinal, put

$$N'_{i,\rho} = \bigcap_{\lambda<\rho} N'_{i,\lambda} \quad (i = 1, 2).$$

Observe that

$$G_i/N'_{i,\rho} = \varprojlim_{\lambda<\rho} G_i/N'_{i,\lambda} \quad (i = 1, 2).$$

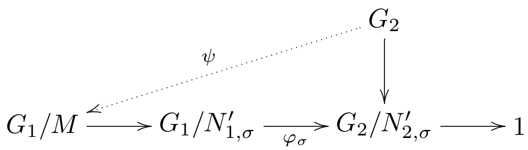
In this case, define

$$\varphi_\rho = \varprojlim_{\lambda<\rho} \varphi_\lambda.$$

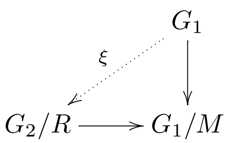
By Theorem 2.6.4, one has that

$$w_0(G_i/N'_{i,\rho}) \leq \sum_{\lambda<\rho} w_0(G_i/N_{i,\lambda}) = w_0(G_i/N_{i,\rho}).$$

If $\rho = \sigma + 1$ for some ordinal σ, we proceed as follows: put $M = N'_{1,\sigma} \cap N_{1,\rho}$ and $P = N'_{2,\sigma} \cap N_{2,\rho}$. Observe that $[N'_{1,\sigma} : M] < \infty$ and $[N'_{2,\sigma} : P] < \infty$. Let the continuous epimorphism $\psi : G_2 \longrightarrow G_1/M$ be a solution to the $\mathcal{E}$-embedding problem for G_2



Set $R = P \cap \mathrm{Ker}(\psi)$. Then ψ induces a natural epimorphism $G_2/R \longrightarrow G_1/M$. Let the continuous epimorphism $\xi : G_1 \longrightarrow G_2/R$ be a solution to the $\mathcal{E}$-embedding problem for G_1



(such a solution exists since $w_0(G_1/M) < w_0(G_2)$). Set $S = \mathrm{Ker}(\xi)$. Therefore ξ induces an isomorphism $\delta : G_1/S \longrightarrow G_2/R$. Set $N'_{1,\rho} = S$, $G'_{2,\rho} = R$, and $\varphi_\rho = \delta$. Then $N'_{1,\rho} \leq N_{1,\rho}$, $N'_{2,\rho} \leq N_{2,\rho}$ and

$$\begin{array}{ccc} G_1/N'_{1\rho} & \xrightarrow{\varphi_\rho} & G_2/N'_{2\rho} \\ \downarrow & & \downarrow \\ G_1/N'_{1,\sigma} & \xrightarrow[\varphi_\sigma]{} & G_2/N'_{2,\sigma} \end{array}$$

commutes. Finally, observe that $w_0(G_1/N'_{1,\rho}) < w_0(G_1)$ and $w_0(G_2/N'_{2,\rho}) < w_0(G_2)$, as desired. $\square$

The following useful special case is obtained by putting $N_i = G_i$ $(i = 1, 2)$.

Corollary 3.5.7 *Let $\mathcal{C}$ be a formation of finite groups. Let G_1 and G_2 be infinite pro-$\mathcal{C}$ groups, with $w_0(G_1) = w_0(G_2)$. Assume that G_1 and G_2 have the strong lifting property over the class of all continuous epimorphisms of pro-$\mathcal{C}$ groups. Then G_1 and G_2 are isomorphic.*

Next we present two results that characterize free pro-$\mathcal{C}$ groups on a set converging to 1 in terms of embedding problems. The first one is about free groups of finite rank. As we shall see in many occasions, the second result is a most useful tool whenever one wants to investigate whether an infinitely generated pro-$\mathcal{C}$ group is free pro-$\mathcal{C}$.

Theorem 3.5.8 *Let $\mathcal{C}$ be a formation of finite groups and let G be a pro-$\mathcal{C}$ group. Assume that $d(G) = m$ is finite. Let $\mathcal{E} = \mathcal{E}_\mathcal{C}$ be the class of all epimorphisms of pro-$\mathcal{C}$ groups. Then, the following two conditions are equivalent*

(a) *G is a free pro-$\mathcal{C}$ group of rank m;*
(b) *Every $\mathcal{E}$-embedding problem for G*

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array}$$

with $d(B) \le d(G)$ and $d(A) \le d(G)$, has a solution.

Proof. (a) $\Rightarrow$ (b) This implication follows immediately from Proposition 2.5.4.

(b) $\Rightarrow$ (a) Consider a free pro-$\mathcal{C}$ group F of rank m, and let $\alpha : F \longrightarrow G$ be a continuous epimorphism. By (b) there exists an continuous epimorphism $\varphi : G \longrightarrow F$ such that $\alpha\varphi = \mathrm{id}_G$. Then φ is a monomorphism, and thus an isomorphism. $\square$

Theorem 3.5.9 *Let $\mathcal{C}$ be a formation of finite groups and let G be a pro-$\mathcal{C}$ group. Assume that $d(G) = \mathfrak{m}$ is infinite. Let $\mathcal{E} = \mathcal{E}_\mathcal{C}$ be the class of all epimorphisms of pro-$\mathcal{C}$ groups. Then, the following two conditions are equivalent*

(a) *G is a free pro-$\mathcal{C}$ group on a set converging to 1 of rank $\mathfrak{m}$;*

(b) *G has the strong lifting property over $\mathcal{E}$.*

Proof. (a) $\Rightarrow$ (b) Let G be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}$ on the set X converging to 1. Then $|X| = w_0(G)$ (see Proposition 2.6.2). Consider the $\mathcal{E}$-embedding problem

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array}$$

with $w_0(B) < w_0(G)$ and $w_0(A) \leq w_0(G)$. We must show that there exists a continuous epimorphism $\bar{\varphi} : G \longrightarrow A$ such that $\alpha\bar{\varphi} = \varphi$. According to Lemma 3.5.4, we may assume that K is finite. Put $X_0 = X \cap \mathrm{Ker}(\varphi)$. Let $\mathcal{U}$ be the collection of all open normal subgroups of B. By our assumptions, $|\mathcal{U}| < \mathfrak{m}$. Observe that, since X converges to 1,

$$|X - \mathrm{Ker}(\varphi)| = \left| X - \bigcap_{U \in \mathcal{U}} \varphi^{-1}(U) \right| = \left| \bigcup_{U \in \mathcal{U}} (X - \varphi^{-1}(U)) \right| = |\mathcal{U}|.$$

Therefore, $|X_0| = \mathfrak{m}$. Let Z be a set of generators of K; since Z is finite, we may choose a subset Y of X_0 such that $|Z| = |Y|$. By Proposition 2.2.2, there exists a continuous section $\sigma : B \longrightarrow A$ of α. Think of K as a subgroup of A. Define $\varphi_1 : X \longrightarrow A$ as a map that sends Y to Z bijectively, and such that $\varphi_1 = \sigma\varphi$ on $X - Y$. Since X is a set converging to 1 and φ and σ are continuous, the mapping φ_1 converges to 1. Therefore, φ_1 extends to a continuous homomorphism $\bar{\varphi} : G \longrightarrow A$ with $\alpha\bar{\varphi} = \varphi$. Finally note that $\bar{\varphi}$ is onto since $\varphi_1(X)$ generates A.

(b) $\Rightarrow$ (a) This follows immediately from Corollary 3.5.7. □

Combining the theorem above with Lemma 3.5.4, we get the following characterization of free pro-$\mathcal{C}$ groups of infinite countable rank.

Corollary 3.5.10 *Let $\mathcal{C}$ be a formation of finite groups and let G be a pro-$\mathcal{C}$ group with $w_0(G) = \aleph_0$. Then G is a free pro-$\mathcal{C}$ group on a countably infinite set converging to 1 if and only if every embedding problem of the form*

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array}$$

has a solution whenever A is finite.

The next result provides another characterization of free pro-$\mathcal{C}$ groups from a slightly different point of view.

Proposition 3.5.11 *Let $\mathcal{C}$ be a formation of finite groups and let G be a pro-$\mathcal{C}$ group. Assume that $d(G) = \mathfrak{m}$ is infinite. Then G is a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}$ if and only if the following condition is satisfied*:

($*$) *every embedding problem of pro-$\mathcal{C}$ groups*

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \big\downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & C & \xrightarrow{\alpha} & D & \longrightarrow & 1, \end{array}$$

with $1 \neq C \in \mathcal{C}$, has $\mathfrak{m}$ different solutions $\psi : G \longrightarrow C$.

Proof. Assume that G is a free pro-$\mathcal{C}$ group on a set X converging to 1 with $|X| = \mathfrak{m}$. Consider an embedding problem for G as above, with C finite. Since D is finite, $U = \mathrm{Ker}(\varphi)$ is open in G. Hence, $X - U$ is finite and $|X \cap U| = \mathfrak{m}$. Since K is finite, there exists an indexing set I of cardinality $\mathfrak{m}$ and a collection $\{X_i\}_{i \in I}$ of distinct subsets of $X \cap U$, each of them of size $|K|$. Let $\sigma : D \longrightarrow C$ be a section of α. For each $i \in I$, define a map $\varphi_i : X \longrightarrow C$ as follows: $\varphi_i = \sigma\varphi$ on $X - U$, φ_i sends X_i to K bijectively (we think of K as a subgroup of C), and $\varphi_i(X \cap U - X_i)) = 1$. Clearly, $\varphi_i(X)$ generates C. Thus φ_i extends to a continuous epimorphism $\psi_i : G \longrightarrow C$ with $\alpha\psi_i = \varphi$. Furthermore, the maps ψ_i $(i \in I)$ are all distinct.

Conversely, assume that condition ($*$) holds. Consider an embedding problem

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \big\downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1, \end{array}$$

where A and B are pro-$\mathcal{C}$ groups and where $w_0(B) < \mathfrak{m}$ and $w_0(A) \leq \mathfrak{m}$. According to Theorem 3.5.9, it suffices to show that such an embedding problem has a solution. By Lemma 3.5.4, we may assume that K is a finite minimal normal subgroup of A. Let $V \triangleleft_o A$ be such that $V \cap K = 1$. Consider the commutative diagram

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \big\downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \\ & & \big\downarrow{\scriptstyle\beta_{|K}} & & \big\downarrow{\scriptstyle\beta} & & \big\downarrow{\scriptstyle\gamma} & & \\ 1 & \longrightarrow & K_V = KV/V & \longrightarrow & A/V & \xrightarrow{\alpha_V} & B/\alpha(V) & \longrightarrow & 1, \end{array}$$

where β and γ are the canonical epimorphisms, α_V is the epimorphism induced by α and $K_V = \mathrm{Ker}(\alpha_V)$. One shows easily that the maps $\alpha, \beta, \alpha_V, \gamma$

form a pullback diagram (see Exercise 2.10.1); moreover, $\beta_{|K}$ is an isomorphism and K_V is minimal normal in A/V.

By assumption, since $A/V \in \mathcal{C}$, there exists an indexing set I with $|I| = \mathfrak{m}$ and distinct continuous epimorphisms $\psi_i : G \longrightarrow A/V$ such that $\alpha_V \psi_i = \gamma\varphi$ ($i \in I$). By definition of pullback, for each $i \in I$, there exists a unique continuous homomorphism $\bar{\varphi}_i : G \longrightarrow A$ such that $\alpha\bar{\varphi}_i = \varphi$ and $\beta\bar{\varphi}_i = \psi_i$. The proof will be finished if we can prove that $\bar{\varphi}_j$ is an epimorphism for some $j \in I$. Observe that for this it suffices to prove the following claim: $\mathrm{Ker}(\varphi) \not\leq \mathrm{Ker}(\psi_j)$, for some $j \in I$. Indeed, if the claim holds, $\psi_j(\mathrm{Ker}(\varphi))$ is a nontrivial normal subgroup of A/V. Hence either $K_V \cap \psi_j(\mathrm{Ker}(\varphi)) = 1$ or $K_V \leq \psi_j(\mathrm{Ker}(\varphi))$, since K_V is minimal normal in A/V. On the other hand, $\alpha_V(\psi_j(\mathrm{Ker}(\varphi))) = (\gamma\varphi)(\mathrm{Ker}(\varphi)) = 1$; so, we deduce that $\psi_j(\mathrm{Ker}(\varphi)) = K_V$. Therefore, $\mathrm{Ker}(\alpha_V\psi_j) = \mathrm{Ker}(\varphi)\mathrm{Ker}(\psi_j)$. Thus, by Lemma 2.10.2, $\bar{\varphi}_j$ is surjective.

It remains to prove the claim. Let $N = \bigcap_{i\in I} \mathrm{Ker}(\psi_i)$. It follows that $w_0(G/N) = \mathfrak{m}$. Indeed, assume that $w_0(G/N) = \mathfrak{n} < \mathfrak{m}$; then G/N is a quotient of a free pro-$\mathcal{C}$ group F of rank $\mathfrak{n}$; so, F would have $\mathfrak{m}$ distinct continuous epimorphisms onto the finite group A, which is plainly impossible, since each such an epimorphism is completely determined by its values on a finite subset of a basis of F. Therefore, $w_0(G/N) = w_0(G) > w_0(B) = w_0(G/\mathrm{Ker}(\varphi))$. This implies that $\mathrm{Ker}(\varphi) \not\leq \mathrm{Ker}(\psi_j)$, for some $j \in I$. □

Next we prove that all free pro-$\mathcal{C}$ groups are in fact free pro-$\mathcal{C}$ groups on some set converging to 1. Nevertheless, it is sometimes more natural and more convenient to describe certain free pro-$\mathcal{C}$ group as being free on a topological space, rather than on a set; this becomes apparent when one studies subgroups of free groups (see Section 8.1).

Proposition 3.5.12 *Let $\mathcal{C}$ be a formation of finite groups and let $F = F_{\mathcal{C}}(X, *)$ be a free pro-$\mathcal{C}$ group on a pointed profinite space $(X, *)$. Then F is a free pro-$\mathcal{C}$ group on a certain set converging to 1. Furthermore, let $\mathcal{R}$ be the collection of all open equivalence relations R on X. Then if $\mathcal{R}$ is finite, so is the rank of F, and if $\mathcal{R}$ is infinite,* $\mathrm{rank}(F) = |\mathcal{R}|$.

Proof. If X is finite, there is nothing to prove. So, we assume from now on that $(X, *)$ is an infinite pointed profinite space. Clearly $|\mathcal{R}| = \rho(X)$, where $\rho(X)$ denotes the cardinality of the set of clopen subsets of X. We seek to prove that $F = F_{\mathcal{C}}(X, *)$ is a free pro-$\mathcal{C}$ group on a set of cardinality $\rho(X)$ converging to 1. Let $\mathcal{E} = \mathcal{E}_{\mathcal{C}}$ be the class of all epimorphisms of pro-$\mathcal{C}$ groups and consider an $\mathcal{E}$-embedding problem

$$\begin{array}{ccccccccc} & & & & & & F & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array} \tag{6}$$

where $w_0(B) < w_0(F)$ and $w_0(A) \leq w_0(F)$. According to the characterization of free pro-$\mathcal{C}$ groups on a set converging to 1 established in Theorem 3.5.9, we must show that there exists a continuous epimorphism $\bar{\varphi} : F \longrightarrow A$ such that $\alpha\bar{\varphi} = \varphi$. By Lemma 3.5.4, we may assume that the kernel K is finite.

Put $Y = \varphi(X)$, and let $\psi : X \longrightarrow Y$ be the restriction of φ to X. Note that ψ is a mapping of pointed spaces, if we think of 1 as the distinguished point of Y. It follows from Proposition 2.6.2 and our hypotheses that $\rho(Y) < \rho(X)$. In particular, if Y is finite, then $\psi^{-1}(y)$ is infinite for some $y \in Y$.

So in any case we may choose points $y_1, \dots, y_m \in Y$, and for each $i = 1, \dots, m$, points $x_{i,0}, \dots, x_{i,n_i} \in \psi^{-1}(y_i)$, none of them equal to $*$, such that $n_1 + \cdots + n_m = |K| - 1$. Represent the set of elements of K as

$$\{1\} \cup \{k_{i,j} \mid i = 1, \dots, m; j = 0, \dots, n_i\}.$$

Choose clopen subsets U and $U_{i,j}$ of X such that $* \in U, x_{i,j} \in U_{i,j}$ $(i = 1, \dots, m; j = 0, \dots, n_i)$ and $X = U \mathbin{\dot\cup} U_{1,0} \mathbin{\dot\cup} \cdots \mathbin{\dot\cup} U_{m,n_m}$. Define

$$\delta : X \longrightarrow K$$

as follows: $\delta(x) = 1$ if $x \in U$ or if $x \in U_{i,0}$ $(i = 1, \dots, m)$, and $\delta(x) = k_{i,j}$ if $x \in U_{i,j}$ $(i = 1, \dots, m; j = 1, \dots, n_i)$. Then δ is a continuous mapping. Next, consider a continuous section

$$\sigma : B \longrightarrow A$$

of α such that $\sigma(1) = 1$ (see Proposition 2.2.2), and define

$$\xi : X \longrightarrow A$$

by $\xi(x) = \delta(x)\sigma(\psi(x))$ for $x \in X$. Plainly, ξ is continuous and $\xi(*) = 1$. Therefore there exists a continuous homomorphism

$$\bar{\xi} : F \longrightarrow A$$

extending ξ. Observe that $\alpha(\bar{\xi}(x)) = \psi(x)$ for all $x \in X$. It follows that $\alpha\bar{\xi} = \xi$. We claim that $\bar{\varphi} = \bar{\xi}$ is the desired solution of the $\mathcal{E}$-embedding problem (6). To verify this claim it remains to show that $\bar{\xi}$ is an epimorphism. Note first that

$$\xi(x_{i,j})\xi(x_{i,0})^{-1} = \delta(x_{i,j})\sigma(\psi(x_{i,j}))(\delta(x_{i,0})\sigma(\psi(x_{i,0})))^{-1} = k_{i,j}$$

$(i = 1, \dots, m; j = 1, \dots, n_i)$; therefore, $K \leq \bar{\xi}(F)$. On the other hand, $\alpha(\bar{\xi}(F)) = B$, and thus $\bar{\xi}(F) = A$, as required. □

The proof of the theorem above is not constructive, in the sense that it does not exhibit an explicit basis of F converging to 1. The following theorem shows that a construction of such a basis cannot be expected. It answers negatively Open Question 3.5.13 in the first edition of this book.

Theorem 3.5.13 *Let X be a profinite space and let $F = F(X)$ be the free pro-$\mathcal{C}$ group on X. There is no basis S of F converging to 1 that can be obtained from X in a canonical way, or more precisely, there is no such S that is left invariant under the action of the group* $\mathrm{Aut}(X)$ *of homeomorphisms from X to X.*

Proof. We prove this by exhibiting a concrete example of a variety $\mathcal{C}$ and a space X such that no basis S of F converging to 1 is left invariant under the action of the group of automorphisms of F induced by the homeomorphisms in $\mathrm{Aut}(X)$.

Choose $\mathcal{C}$ to be the variety of all finite p-groups, where p is a fixed prime number. Observe that the Frattini quotient $F/\Phi(F)$ of F is a vector space over the field $\mathbf{F}_p$ with p elements and it is also the free pro-$\underline{\mathcal{C}}$ group on the space X, where $\underline{\mathcal{C}}$ is the variety of all finite abelian p-groups of exponent p (the vector spaces of finite dimension over $\mathbf{F}_p$). A basis S of F converging to 1 can be consider to be also a basis of $F/\Phi(F)$ converging to 1; moreover every $\varphi \in \mathrm{Aut}(X)$ induces a continuous automorphism of $F/\Phi(F)$; hence we may replace F by $F/\Phi(F)$.

Consider the Pontryagin dual $\mathrm{Hom}(F/\Phi(F), \mathbf{F}_p)$ of $F/\Phi(F)$. Under this duality, a basis S of $F/\Phi(F)$ converging to 1 is transformed into an ordinary basis of the discrete vector space $\mathrm{Hom}(F/\Phi(F), \mathbf{F}_p) = C(X, \mathbf{F}_p)$ over the field $\mathbf{F}_p$; furthermore, every $\varphi \in \mathrm{Aut}(X)$ is transformed into an automorphism of $C(X, \mathbf{F}_p)$. Therefore, it suffices to prove that, after an appropriate choice of X, there exists no basis of the vector space $C(X, \mathbf{F}_p)$ which is left invariant under the action of $\mathrm{Aut}(X)$. Fix a prime q, and let $X = \mathbf{Z}_q$. The result will follow if we prove the following stronger assertion:

Let $f : X \longrightarrow \mathbf{F}_p$ be a nonconstant continuous function. Then the transforms of f under $\mathrm{Aut}(X)$ *are linearly dependent.*

For simplicity we restrict ourselves to the case $p = 2$ (the argument can be easily extended to any prime p). Consider the decomposition

$$\mathbf{Z}_q = \varprojlim_{n \in \mathbf{N}} \mathbf{Z}/q^n\mathbf{Z}.$$

By Lemma 1.1.16, f factors through $\mathbf{Z}/q^{n_0}\mathbf{Z}$, for some $n_0 \in \mathbf{N}$, i.e., there exists $\tilde{f} : \mathbf{Z}/q^{n_0}\mathbf{Z} \longrightarrow \mathbf{F}_2 = \{0, 1\}$ such that

$$f = \tilde{f}\varphi_{n_0},$$

where $\varphi_{n_0} : \mathbf{Z}_q \longrightarrow \mathbf{Z}/q^{n_0}\mathbf{Z}$ is the projection.

Let a be the number of elements $z \in \mathbf{Z}/q^{n_0}\mathbf{Z}$ such that $\tilde{f}(z) = 0$, and let b be the number of elements $z \in \mathbf{Z}/q^{n_0}\mathbf{Z}$ such that $\tilde{f}(z) = 1$. Note $a + b = q^{n_0}$. Since f is nonconstant, $a, b > 0$. In fact we may assume $a, b > 1$: simply replace $\mathbf{Z}/q^{n_0}\mathbf{Z}$ by $\mathbf{Z}/q^{n_0+1}\mathbf{Z}$ (this has the effect of multiplying a and b by q). Now consider the set T of functions obtained by transforming $\tilde{f}$ by the permutations of $\mathbf{Z}/q^{n_0}\mathbf{Z}$. Then

$$|T| = \frac{q^{n_0}!}{a!b!} = \binom{q^{n_0}}{a}.$$

Since $a > 1$, we get $|T| > q^{n_0}$. Since

$$\dim C(\mathbf{Z}/q^{n_0}\mathbf{Z}, \mathbf{F}_2) = q^{n_0},$$

we deduce that the elements of T are linearly dependent. Finally observe that every permutation of $\mathbf{Z}/q^{n_0}\mathbf{Z}$ is induced by a homeomorphism

$$\mathbf{Z}_q \longrightarrow \mathbf{Z}_q,$$

i.e., an element of $\mathrm{Aut}(X)$. This proves the above assertion and the theorem. □

Exercise 3.5.14 Let $\mathcal{C}$ be a nontrivial formation of finite groups and X a set. Prove

(a) If $X \neq \emptyset$ is finite, $|F_{\mathcal{C}}(X)| = 2^{\aleph_0}$.
(b) Let C be a finite cyclic group in $\mathcal{C}$, and let $G = \prod_X C$ be the direct product of $|X|$ copies of C. Then G can be generated by a set converging to 1 of cardinality $|X|$.
(c) If X is infinite and let F be the free pro-$\mathcal{C}$ group on the set X converging to 1, then $|F| = 2^{|X|}$. (Hint: use Proposition 2.6.2.)
(d) Assume that X is infinite and let $\Phi = \Phi(X)$ be a free abstract group on X. Then the pro-$\mathcal{C}$ completion of Φ is a free pro-$\mathcal{C}$ group of rank $2^{|X|}$. (Hint: see Exercise 3.3.3.)
(e) Let $\mathfrak{m}$ be an infinite cardinal and let p be a fixed prime number. Consider the direct sum $A = \bigoplus_{\mathfrak{m}} \mathbf{Z}/p\mathbf{Z}$ of $\mathfrak{m}$ copies of $\mathbf{Z}/p\mathbf{Z}$. Then $d(\widehat{A}) = 2^{\mathfrak{m}}$.
(f) Let Y be an infinite topological space with the discrete topology. Show that
$$|F_{\mathcal{C}}(Y)| = 2^{2^{|Y|}}.$$

In Proposition 3.3.9 we saw that an inverse limit of free pro-$\mathcal{C}$ groups is a free pro-$\mathcal{C}$ group if the canonical mappings in the inverse system send bases to bases. As we shall exhibit later (see Example 9.1.14), a general inverse limit G of free pro-$\mathcal{C}$ groups need not be free pro-$\mathcal{C}$. However, in the following theorem we show that if, in addition, G has a countable fundamental system of neighborhoods of the identity (i.e., $w_0(G) = \aleph_0$), then G is free pro-$\mathcal{C}$.

Theorem 3.5.15 *Let*

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

be an inverse limit of a surjective inverse system of free pro-$\mathcal{C}$ groups (F_i, φ_{ij}) indexed by a poset I. Assume that G admits a countable set of generators converging to 1 (i.e., G is second countable as a topological space). Then G is a free pro-$\mathcal{C}$ group.

Proof. Suppose first that G is finitely generated. Then the free groups F_i have finite rank bounded by $d(G)$, the minimal number of generators of G. It follows that there exists some $i_o \in I$ such that $\operatorname{rank}(F_i) = \operatorname{rank}(F_{i_o})$ if $i \geq i_o$. Therefore, by the Hopfian property (see Proposition 2.5.2), $\varphi_{ii_o} : F_i \longrightarrow F_{i_o}$ is an isomorphism for each $i \geq i_o$. Thus $G \cong F_{i_o}$ is a free pro-$\mathcal{C}$ group.

Assume next that G admits an infinite countable set of generators converging to 1. Let $\mathcal{E} = \mathcal{E}_{\mathcal{C}}$ be the class of all epimorphisms of pro-$\mathcal{C}$ groups. Then, according to Corollary 3.5.10, it suffices to prove that every $\mathcal{E}$-embedding problem for G of the form

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array}$$

has a solution, whenever A is a finite group.

Denote by

$$\varphi_r : G \longrightarrow F_r$$

the canonical epimorphism. Since B is finite, there exists some $r \in I$ and an epimorphism

$$\psi_r : F_r \longrightarrow B$$

such that $\varphi = \psi_r \varphi_r$ (see Lemma 1.1.16). Since G is not finitely generated, we may choose r in such a way that $\operatorname{rank}(F_r) > |A|$. By Theorem 3.5.8, there exists an epimorphism $\mu : F_r \longrightarrow A$ such that $\alpha\mu = \psi_r$. Therefore, $\mu\varphi_r : G \longrightarrow A$ is the desired solution to the above embedding problem. $\square$

3.6 Open Subgroups of Free Pro-$\mathcal{C}$ Groups

In this section we begin the study of the structure of closed subgroups of free pro-$\mathcal{C}$ groups. Unlike the situation for subgroups of abstract free groups, a closed subgroup of a free pro-$\mathcal{C}$ group is not necessarily a free pro-$\mathcal{C}$ group. For example, $\mathbf{Z}_p$ is a closed subgroup of the free profinite group of $\widehat{\mathbf{Z}}$, but obviously $\mathbf{Z}_p$ is not a free profinite group. Nevertheless, we shall describe several types of closed subgroups of a free pro-$\mathcal{C}$ group, and we shall see that in some cases they are free pro-$\mathcal{C}$. We revisit this topic at other places in this book; in particular, in Chapter 7, where we deal with subgroups of free pro-p groups, and in Chapter 8, where we study normal subgroups of free pro-$\mathcal{C}$ groups.

Before we state the next theorem, we fix notation and recall some results about subgroups of abstract free groups. For the details one can consult Magnus, Karras and Solitar [1966], Lyndon and Schupp [1977], or Serre [1980], for example. Let D be an abstract free group on a set X, and let L be a subgroup of D. Recall that a right transversal T of L in D is a complete system of representatives of the right cosets of L in D, so that $D = \cup_{t\in T} Lt$; we shall assume that $1 \in T$. Write $t \in T$ as a reduced word in term of the elements of X, i.e., $t = x_1^{\epsilon_1} \cdots x_r^{\epsilon_r}$ for some $x_1, \dots, x_r \in X$, with $\epsilon_i = \pm 1$ for all $i = 1, \dots, r$, and $\epsilon_i = \epsilon_{i+1}$ if $x_i = x_{i+1}$ $(i = 1, \dots, r-1)$. We refer to the elements $x_1^{\epsilon_1} \cdots x_i^{\epsilon_i}$ $(i = 0, \dots, r)$ as the initial segments of $t = x_1^{\epsilon_1} \cdots x_r^{\epsilon_r}$. We say that the transversal T is a *right Schreier transversal* if whenever t is in T, so is any initial segment of t. Every subgroup L of D admits a right Schreier transversal. A final piece of notation: if $f \in D$, denote by $\tilde{f}$ the unique element $\tilde{f} \in T$ such that $L\tilde{f} = Lf$. Then one has the following theorem due to Nielsen and Schreier.

Theorem 3.6.1 *Let D be an abstract free group on a set X, L a subgroup of D, and let T be a right Schreier transversal of L in D. Then L is a free group on the set*

$$\{tx(\widetilde{tx})^{-1} \mid x \in X, t \in T, tx(\widetilde{tx})^{-1} \neq 1\}.$$

Furthermore, if L has finite index in D, then

$$\operatorname{rank}(L) - 1 = [D : L](\operatorname{rank}(D) - 1).$$

Theorem 3.6.2 *Assume that $\mathcal{C}$ is an extension closed variety of finite groups (respectively, an NE-formation of finite groups). Let F be a free pro-$\mathcal{C}$ group on a set X converging to 1, and let H be an open (respectively, open normal) subgroup of F. Then*

(a) *The set*
$$Z = \{tx(\widetilde{tx})^{-1} \mid x \in X, t \in T, tx(\widetilde{tx})^{-1} \neq 1\},$$
converges to 1, where T is an appropriate right transversal of H in F; moreover, H is a free pro-$\mathcal{C}$ group on the set Z.

(b) *If* $\operatorname{rank}(F)$ *is infinite, then* $\operatorname{rank}(H) = \operatorname{rank}(F)$; *while if* $\operatorname{rank}(F)$ *is finite,then so is* $\operatorname{rank}(H)$, *and*

$$\operatorname{rank}(H) - 1 = [F : H](\operatorname{rank}(F) - 1).$$

Proof. Let D be the abstract subgroup of F generated by X. By Corollary 3.3.14 and Proposition 3.3.15, D is an abstract free group with basis X. Choose a Schreier transversal T of $D \cap H$ in D.

Case 1. $X = \{x_1, \dots, x_n\}$ is finite.

As pointed out above, $D \cap H$ is a free abstract group. By Proposition 3.2.2, $\overline{D \cap H} = H$. By Lemmas 3.1.4, 3.2.4 and 3.2.6, H is the pro-$\mathcal{C}$ completion of $D \cap H$; hence H is a free pro-$\mathcal{C}$ group. Then, by Theorem 3.6.1,

$$\{tx(\widetilde{tx})^{-1} \mid x \in X, t \in T, tx(\widetilde{tx})^{-1} \neq 1\}$$

is a basis of $D \cap H$, and so of H (see Proposition 3.3.6). Therefore, using again Theorem 3.6.1, $\operatorname{rank}(H) - 1 = [F : H](\operatorname{rank}(F) - 1)$, as desired.

Case 2. X is an infinite set.

By Proposition 3.3.12, we may express the free pro-$\mathcal{C}$ group $F = F_{\mathcal{C}}(X)$ on the set X converging to 1 as an inverse limit

$$F = \varprojlim_{j\in J} F_{\mathcal{C}}(X_j),$$

with $[F_{\mathcal{C}}(X_j) : \varphi_j(H)] = [F : H]$, for every $j \in J$, where each X_j is a finite subset of X, and $\varphi_j : F \longrightarrow F_{\mathcal{C}}(X_j)$ denotes the canonical epimorphism. Let D_j be the abstract subgroup of $F_{\mathcal{C}}(X_j)$ generated by X_j ($j \in J$). Therefore, $\varphi_j(T) = \{\varphi_j(t) \mid t \in T\}$ is a Schreier transversal of the subgroup $D_j \cap \varphi_j(H)$ in D_j ($j \in J$). Put $\tilde{X} = X \cup \{1\}$ and $\tilde{X}_j = X_j \cup \{1\}$ ($j \in J$). Then $F_{\mathcal{C}}(X_j) = F_{\mathcal{C}}(\tilde{X}_j, 1)$. By Case 1, $\varphi_j(H)$ is a free pro-$\mathcal{C}$ group on the finite pointed space

$$(Y_i, 1) = (\{x\varphi_j(t)(\widetilde{x\varphi_j(t)})^{-1} \mid x \in \tilde{X}_j, t \in T\}, 1).$$

Observe that $\varphi_{jk}(\tilde{Y}_j, 1) = (\tilde{Y}_k, 1)$ ($j \succeq k$), and that

$$H = \varprojlim_{j\in J} \varphi_j(H).$$

Hence, by Proposition 3.3.9, H is a free pro-$\mathcal{C}$ group on the pointed topological space

$$(Y, 1) = (\varprojlim_{j\in J} Y_j, 1).$$

It remains to prove that Y is the one-point compactification of the set Z in the statement. Clearly Z is a discrete subspace of F since X is discrete and T is finite. Moreover, $Z \cup \{1\}$ is compact (it is the continuous image of the compact space $(X \cup \{1\}) \times T$), in fact, it is the one-point compactification of Z. Since $\varphi_j(Z \cup \{1\}) = \tilde{Y}_j$ ($j \in J$), we infer that $Z \cup \{1\} = Y$ (see Corollary 1.1.8). This proves the theorem. □

Corollary 3.6.3 *Let G be a finitely generated profinite group with* $\mathrm{d}(G) = d$ *and let $U \leq_o G$. Then U is also finitely generated as a profinite group and* $\mathrm{d}(U) \leq 1 + [G : U](d - 1)$.

Proof. Consider a free profinite group F of rank d and an epimorphism

$$\varphi : F \longrightarrow G.$$

Then $\varphi(\varphi^{-1}(U)) = U$. So the result follows from Theorem 3.6.2 applied to the open subgroup $\varphi^{-1}(U)$ of F. □

A subgroup H of a group G is called *subnormal* if there exists a finite chain of subgroups of G

$$H = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 = G.$$

If G is profinite and H is closed, we only refer to H as subnormal if there is a chain as above with every G_i closed.

Corollary 3.6.4

(a) *For* $r, i \in \mathbf{N}$, *define* $\mathrm{T}(r,i) = 1 + i(r-1)$. *If* $r, i, j \in \mathbf{N}$, *then*

$$\mathrm{T}(\mathrm{T}(r,i), j) = \mathrm{T}(r, ij).$$

(b) *Let* $\mathcal{C}$ *be an NE-formation of finite groups. Let* F *be a free pro-*$\mathcal{C}$ *group of finite* rank r, *and let* H *be an open subnormal subgroup of* F. *Then* H *is a free pro-*$\mathcal{C}$ *group of* rank $1 + [F : H](r-1)$.

Proof. Part (a) is a routine calculation. Part (b) follows from the theorem and an easy induction. □

3.7 Notes, Comments and Further Reading

Profinite topologies are used sometimes to express some algebraic facts in a succinct manner. For example, an abstract group G is called LERF or *subgroup separable* if every finitely generated subgroup of G is closed in the profinite topology of G (cf. Scott [1978]). In Hall [1949] Theorem 5.1, it is proved that finitely generated subgroups of abstract free groups are closed in the profinite topology; see also Hall [1950]. For a study of the induced topology on the Fitting subgroup of certain groups, see Pickel [1976] and Kilsch [1986].

Lemma 3.1.5 and Corollary 3.1.6 appear in Ribes and Zalesskii [1994]. Corollary 3.2.8 was proved by Dixon, Formanek, Poland and Ribes [1982]. Theorem 3.2.9 appears in Fried and Jarden [2008]. For polycyclic groups with isomorphic finite quotients see Grunewald, Pickel and Segal [1980].

Free pro-$\mathcal{C}$ groups appear in Iwasawa [1953], where $\mathcal{C}$ is a variety of finite groups, although he does not use the name 'free pro-$\mathcal{C}$'. In the same paper (Theorem 8) Iwasawa proves a precursor of the results of Douady and Harbater mentioned in Example 3.3.8(e): let F be an algebraically closed countable field and let K be the maximal solvable extension of $F(T)$; then the Galois group of the extension $K/F(T)$ is a free prosolvable group of countable rank. The first explicit reference to the universal property of freeness for pro-p groups seems to appear in the first edition of Serre's Cohomologie Galoisienne. The first systematic study of free pro-$\mathcal{C}$ groups over topological spaces was began by Gildenhuys and Lim [1972]. At the time it was known, using cohomological methods, that every free pro-p group on a topological space is free on a set converging to 1 (Tate); see Section 7.6. Proposition 3.5.12, showing that this is also the case for general pro-$\mathcal{C}$ groups, was proved by Mel'nikov [1980]. Proposition 3.3.9 appears in Gildenhuys and Lim [1972]. Proposition 3.3.12 was established in Gildenhuys and Ribes [1973]. A version of Theorem 3.3.16 is shown in Iwasawa [1953].

The embedding problem, as indicated in Remark 3.5.2, seems to have been posed first in Brauer [1932]. The literature about the inverse problem of

Galois theory is very extensive. Open Question 3.5.3 has been partially answered in many special cases. Shafarevich [1954] answered it for finite solvable groups (this paper had a difficulty related to the prime number 2, but Shafarevich indicated how to overcome this difficulty shortly after); see Schmidt and Wingberg [1998] for a simplified proof of Shafarevich's result. The book of Matzat [1987] describes the construction of field extensions corresponding to some finite simple groups. See Pop [1996] for the study of embedding problems over certain fields. For a general survey of results and methods see Serre [1992] and Völklein [1996].

Iwasawa [1953] makes a pioneering use of embedding problems for groups to characterize free pro-$\mathcal{C}$ groups of countable rank (see Corollary 3.5.10). This was generalized by Mel'nikov [1978] (see Theorem 3.5.9).

Proposition 3.5.11 was proved by Chatzidakis in her 1984 thesis and appears in Chatzidakis [1998]; this paper contains several other results on free profinite groups. In Jarden [1995], profinite groups with solvable finite embedding problems (i.e., embedding problems such as (1) of Section 3.5, where A is finite) are studied. Theorem 3.5.13 was proved by J-P. Serre (private communication) to answer negatively Open Question 3.5.13 in the first edition of the present book. Theorem 3.5.15 is due to Mel'nikov [1980]. Theorem 3.6.1 appears in Binz, Neukirch and Wenzel [1971]; see a different proof, independent of the Kurosh theorem for abstract groups, in Appendix D, Theorem D.2.2.

Let F be a free nonabelian pro-p group; Zubkov [1987] proves that F cannot be embedded as a closed subgroup of $\mathrm{GL}_2(R)$, if $p \neq 2$ and R is a commutative profinite ring; Barnea and Larsen [1999] show the same result for $\mathrm{GL}_n(F)$, if F is a local field.

3.7.1 A Problem of Grothendieck on Completions

Assume that $\varphi : G_1 \longrightarrow G_2$ is a homomorphism of finitely generated residually finite abstract groups such that the corresponding homomorphism $\widehat{\varphi} : \widehat{G}_1 \longrightarrow \widehat{G}_2$ of the profinite completion is an isomorphism.

Question: Is φ necessarily an isomorphism?

This question was posed in Grothendieck [1970] for groups G_1 and G_2 which in addition are finitely presented. Finite presentability is a natural condition for the groups Grothendieck was studying, namely fundamental groups of certain complex varieties which are compact and locally simply connected; such fundamental groups are finitely presented.

Here we indicate some results related to this question as well as some references. The motivation of Grothendieck was the study of the functor induced by φ

$$\varphi^* : \mathrm{Rep}_A(G_2) \longrightarrow \mathrm{Rep}_A(G_1),$$

where A is a commutative ring and $\mathrm{Rep}_A(G)$ stands for the category of finitely presented A-modules on which the group G operates. Grothendieck [1970], Theorem 1.2, proved that if $\widehat{\varphi}$ is an isomorphism, then φ^* is an equivalence of categories. In this connection see also Lubotzky [1980].

In Platonov and Tavgen [1986] an example was found that answers negatively the above question. This example is based on a construction by Higman [1951] of an infinite finitely presented group with no nontrivial finite quotients. Let F be a free abstract group on a basis $\{x_1, x_2, x_3, x_4\}$. Let N be the smallest normal subgroup of F containing the elements $x_2x_1x_2^{-1}x_1^{-2}, x_3x_2x_3^{-1}x_2^{-2}, x_4x_3x_4^{-1}x_3^{-2}, x_1x_4x_1^{-1}x_4^{-2}$. The group constructed by Higman is F/N. Denote by Δ the diagonal subgroup of the direct product $F \times F$, and consider the subgroup $G_1 = (N \times \{1\})\Delta$ of $G_2 = F \times F$. Then Platonov and Tavgen show that the inclusion $G_1 \longrightarrow G_2$ induces an isomorphism $\widehat{G}_1 \longrightarrow \widehat{G}_2$.

Further examples with negative answers to the question above have been given in Bass and Lubotzky [2000] and Pyber [2004]. All these examples involve groups which do not appear to be finitely presented. Examples with negative answer to Grothendieck's question, i.e., with groups G_1 and G_2 that are finitely presented, are given in Bridson and Grunewald [2004].

Platonov and Tavgen [1990] contains several results showing that in some interesting cases the above question has a positive answer. For example they prove

Theorem 3.7.1 *The above question has a positive answer if G_2 is a subgroup of $\mathrm{SL}_2(K)$, where K is either the field of real or rational numbers.*

In connection with Theorems 3.2.7 and Corollary 3.2.8, one may ask

Open Question 3.7.2 *What pro-$\mathcal{C}$ groups are pro-$\mathcal{C}$ completions of finitely generated abstract groups?*

For partial answers to this question see Segal [2001], and Kassabov and Nikolov [2006].

4 Some Special Profinite Groups

4.1 Powers of Elements with Exponents from $\widehat{\mathbf{Z}}$

Let G be a profinite group and $x \in G$. Since $\widehat{\mathbf{Z}}$ is a free profinite group on $\{1\}$, there is a unique epimorphism

$$\varphi : \widehat{\mathbf{Z}} \longrightarrow \overline{\langle x \rangle}$$

such that $\varphi(1) = x$. Given $\lambda \in \widehat{\mathbf{Z}}$, define $x^\lambda = \varphi(\lambda)$.

Consider the decomposition of $\widehat{\mathbf{Z}}$ as the direct product of it p-Sylow subgroups, $\widehat{\mathbf{Z}} = \prod_p \mathbf{Z}_p$, after identifying the group of p-adic integers $\mathbf{Z}_p$ with the p-Sylow subgroup of $\widehat{\mathbf{Z}}$. If 1 denotes the canonical generator of $\widehat{\mathbf{Z}}$, then 1 can be thought of as infinite tuple $1 = (1_p)$, where 1_p denotes the canonical generator of $\mathbf{Z}_p$, for each prime p. Moreover, $1 = 1_p + 1_{p'}$, where $1_{p'}$ is the canonical generator of the p'-Hall subgroup $\prod_{q \neq p} \mathbf{Z}_q$.

Lemma 4.1.1 *Let G be a profinite group. Let $x, y \in G$ and $\lambda, \mu \in \widehat{\mathbf{Z}}$. Then,*

(a) *If $n_1, n_2, \ldots \in \mathbf{Z}$ is a sequence of integers converging to λ in $\widehat{\mathbf{Z}}$, then*

$$\lim_{i \to \infty} x^{n_i} = x^\lambda.$$

(b) *If x and y commute, then $(xy)^\lambda = x^\lambda y^\lambda$.*
(c) *$x^{\lambda+\mu} = x^\lambda x^\mu$. In particular, $x = x^{1_p} x^{1_{p'}}$.*
(d) *x^{1_p} is a generator of the p-Sylow subgroup of $\overline{\langle x \rangle}$.*

Proof. Part (a) is clear since $\widehat{\mathbf{Z}}$ and $\overline{\langle x \rangle}$ are metric spaces. Parts (b) and (c) are obviously true if the exponents are integers; so the result follows from (a). Part (d) is just the fact that the continuous epimorphism φ above maps the p-Sylow subgroup of $\widehat{\mathbf{Z}}$ onto the p-Sylow subgroup of $\overline{\langle x \rangle}$. □

We recall that a *net* $\{x_i\}$ in a topological space X consists of collection of elements x_i of X indexed by a directed poset $\{I, \preceq\}$. Such a net *converges* to an element x of X if for each neighborhood U of x there exists some $j \in I$ such that $x_k \in U$ whenever $k \succeq j$. A point $y \in X$ is a cluster point of this net if for every neighborhood U of y and each $i \in I$, there is some $j \in I$ with

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4_4,

$j \succeq i$ and $x_j \in U$. It is well-known that X is compact if and only if every net in X has a subnet converging to a point in X.

Let G be a profinite group and p a prime number. We say that an element $x \in G$ is a *p-element* if it generates a pro-p subgroup.

Lemma 4.1.2 *Let G be a profinite group and $\{x_i\}$ a net in G that converges to a p-element x of G. Then $\{x_i^{1_p}\}$ is a net of p-elements of G converging to x.*

Proof. It suffices to show that for any element $y \in G$ and any $U \triangleleft_o G$, one has that $yU = xU$ implies $y^{1_p}U = xU$. To see this, remark first that by Lemma 4.1.1, if $yU = xU$, then $1U = x^{-1}yU = x^{-1}y^{1_p}y^{1_{p'}}U$. Next observe that $y^{1_p}U \in \langle yU \rangle = \langle xU \rangle$; hence $x^{-1}y^{1_p}U$ is a p-element. Therefore, $y^{1_{p'}}U$ is both p-element and a p'-element in the finite group G/U, i.e., $y^{1_{p'}}U = 1U$. Thus $yU = y^{1_p}U$. □

4.2 Subgroups of Finite Index in a Profinite Group

Nikolov and Segal [2007a, 2007b] have proved that the topological structure of a finitely generated profinite group is completely determined by its algebraic structure; more precisely, they prove that the subgroups of finite index of such a group are precisely its open subgroups. The purpose of this section is to present a relatively short proof of this result for a smaller class of groups that includes all prosupersolvable groups and in particular all pro-p groups.

We say that a profinite group G is *strongly complete* if every subgroup of finite index is open. Equivalently, G is strongly complete if it coincides with its profinite completion (thinking of G as an abstract group): $\widehat{G} = G$. It is not hard to find examples of profinite groups that are not strongly complete (see Example 4.2.12); the result of Nikolov and Segal says that none of them are among the finitely generated ones.

Throughout this section we use the following notation, some of it new. Let

$$w = w(x_1, \dots x_n) = \prod_{i=1}^{s} x_{j_i}^{\varepsilon_i} \quad (j_i \in \{1, \dots, n\}, \varepsilon_i = \pm 1)$$

be a group word on the variables $x_1, \dots x_n$; we think of w as representing an element of the free abstract group with basis $x_1, \dots x_n$. For any group G, we denote the set of all w-values in G by

$$\mathfrak{w}(G) = \{w(g_1, \dots, g_n) \mid g_1, \dots, g_n \in G\}.$$

The *verbal subgroup* $w(G)$ of G associated with w is defined to be the subgroup of G generated algebraically by the set $\mathfrak{w}(G)$,

$$w(G) = \langle w(g_1, \dots, g_n) \mid g_1, \dots, g_n \in G \rangle = \langle \mathfrak{w}(G) \rangle.$$

If $w = c = [x, y] = x^{-1}y^{-1}xy$ is the commutator word on x, y, we have that

$$\mathfrak{c}(G) = \{[g, h] = g^{-1}h^{-1}gh \mid g, h \in G\}$$

is the set of all commutators of G; and $c(G) = [G, G]$ is the commutator subgroup of G as an abstract group, i.e., $[G, G]$ consists of all elements of G that can be written as a finite product of commutators; and $\overline{[G, G]}$ is its closure in G.

For a subset Y of G, $\mathrm{Pr}_t(Y)$ is the set of all products of the form $y_1^{\varepsilon_1} \cdots y_t^{\varepsilon_t}$, where t is a natural number, $\varepsilon_i = \pm 1$, and $y_1, \dots, y_t \in Y$.

Let G be a profinite group and let $w = w(x_1, \dots, x_n)$ be a group word; then for each $g \in w(G)$, there is some natural number t such that $g \in \mathrm{Pr}_t(\mathfrak{w}(G))$; clearly this number t depends on g, on G and on w. If there exist such a t which is independent of the element $g \in w(G)$, i.e., if

$$w(G) = \mathrm{Pr}_t(\mathfrak{w}(G)),$$

then we say that w has (at most) *width* t in G; if no such t exists, we say that w has infinite width. For some types of finitely generated profinite groups and some group words w, there is a number t valid for all g, which depends only on the minimal number $d(G)$ of (topological) generators of those groups G and on w. We are interested in this because of the following result.

Lemma 4.2.1 *Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups and let w be a group word. The following conditions are equivalent*:

(a) *For every finitely generated pro-$\mathcal{C}$ group G, $w(G)$ is closed*;
(b) *There exists an integer-valued function f such that for each natural number k and for each group $H \in \mathcal{C}$ that can be generated by k elements, one has*

$$w(H) = \mathrm{Pr}_{f(k)}(\mathfrak{w}(H)),$$

i.e., for each k-generated group $H \in \mathcal{C}$, the word w has width $f(k)$ in H.

Proof. Note that for a profinite group G, the set $\mathfrak{w}(G)$ is compact, hence so is $\mathrm{Pr}_r(\mathfrak{w}(G))$, for each r. Assume that condition (b) holds, and let G be a finitely generated pro-$\mathcal{C}$ group with $d(G) = d$. Express G as an inverse limit of finite quotient groups

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

with canonical epimorphisms $\varphi_i : G \longrightarrow G_i$.

Clearly

$$\overline{w(G)} = \varprojlim_{i \in I} w(G_i)$$

and $\varphi_i(\mathrm{Pr}_t(\mathfrak{w}(G))) = \mathrm{Pr}_t(\mathfrak{w}(G_i))$, for each natural number t. By (b),

$$\mathrm{Pr}_{f(d)}(\mathfrak{w}(G_i)) = w(G_i).$$

Hence $\mathrm{Pr}_{f(d)}(\mathfrak{w}(G))$ is dense in $\overline{w(G)}$, according to Lemma 1.1.7. Since $\mathrm{Pr}_{f(d)}(\mathfrak{w}(G))$ is closed, it follows that $\mathrm{Pr}_{f(d)}(\mathfrak{w}(G)) = \overline{w(G)}$. Plainly,

$$\mathrm{Pr}_{f(d)}(\mathfrak{w}(G)) \subseteq w(G);$$

therefore $w(G) = \overline{w(G)}$.

Suppose now that (a) holds. Let k be a natural number and let F be the free pro-$\mathcal{C}$ group of rank k. Since by our assumption $w(F) = \overline{w(F)}$ is a profinite group which is algebraically generated by $\mathfrak{w}(F)$, it follows from Lemma 2.4.6 that $w(F) = \mathrm{Pr}_m(\mathfrak{w}(F))$, for some natural number m. Define $f(k) = m$. Now, if H is a group in $\mathcal{C}$ that can be generated by k elements, then there is an epimorphism $\varphi : F \longrightarrow H$; consequently $w(H) = \varphi(w(F)) = \varphi(\mathrm{Pr}_{f(k)}(\mathfrak{w}(F))) = \mathrm{Pr}_{f(k)}(\mathfrak{w}(H))$. □

In Nikolov and Segal [2007a, 2007b] they prove the existence of a function, for the class of all finite groups, such as the one described in Lemma 4.2.1. This is the basis of the following

Theorem 4.2.2 *Let G be a finitely generated profinite group. Then every subgroup of G of finite index is open, i.e., G is strongly complete.*

We refer the reader to Nikolov and Segal [2007a, 2007b] for a complete proof of this theorem that depends on the classification of finite simple groups.

Instead, we offer here a relatively short proof of Theorem 4.2.2 for a subclass of prosolvable groups; this class includes all prosupersolvable groups and in particular all pro-p groups. We start with the following

Proposition 4.2.3 *Let G be a profinite group and let N be a subgroup (not necessarily closed) of G of finite index. Then $[G : N]$ divides $\#G$.*

Proof. Replacing N by its core N_G, we may assume that N is normal. Let p be a prime divisor of $[G : N]$. We assert that then p is also a divisor of $\#G$. Indeed, choose $x \in G - N$ such that $x^p \in N$. Then x has order p in the group $\overline{\langle x\rangle}/\overline{\langle x\rangle} \cap N$. Now, $\overline{\langle x\rangle} \cap N$ is open in $\overline{\langle x\rangle}$. Indeed, put $t = [\overline{\langle x\rangle} : \overline{\langle x\rangle} \cap N]$; then

$$\overline{\langle x^t\rangle} \leq \overline{\langle x\rangle} \cap N,$$

and clearly $\overline{\langle x^t\rangle}$ is open in $\overline{\langle x\rangle}$. Therefore p divides $\#\overline{\langle x\rangle}$, and so p divides $\#G$ (see Proposition 2.3.2), proving the assertion.

Next, let p^n be the largest power of p dividing $[G : N]$; we must show that p^n also divides $\#G$. Assume on the contrary that the largest power of p dividing $\#G$ is p^m, with $1 \leq m < n$. Since m is finite, there exists an open subgroup U of G such that p^m divides $[G : U]$; so $p \nmid \#U$. Hence, by the above assertion, $p \nmid [U : U \cap N]$. Therefore p^m is the largest power of p dividing $[G : U \cap N]$. This contradicts the fact that p^n divides $[G : U]$. □

Corollary 4.2.4 *Let G be a prosolvable group, and let N be a normal subgroup (not necessarily closed) of G of finite index. Then G/N is a finite solvable group.*

Proof. Let p be a prime number. It suffices to prove that G/N has a p-complement (cf. Hall [1959], Theorem 9.3.3). According to Proposition 2.3.10, $G = S_pS_{p'}$, where S_p is a p-Sylow subgroup and $S_{p'}$ a p'-Hall subgroup of G. Then

$$G/N = S_pS_{p'}N/N = (S_pN/N)(S_{p'}N/N).$$

By Proposition 4.2.3 $S_pN/N \cong S_p/N \cap S_p$ is a finite p-group and $S_{p'}N/N \cong S_{p'}/N \cap S_{p'}$ a finite p'-group; hence S_pN/N is a p-Sylow subgroup of G/N and $S_{p'}N/N$ a p-complement. □

Proposition 4.2.5 *Let A be a finitely generated abelian profinite group. Then every subgroup N of finite index in G is open.*

Proof. We may assume that A is a free proabelian group of finite rank, say n. Then $A = \bigoplus_{i=1}^n \overline{\langle a_i \rangle}$ where $\overline{\langle a_i \rangle} = \widehat{\mathbf{Z}}$. Let N be a subgroup of A of index t. Then $tA = \bigoplus_{i=1}^n \overline{\langle ta_i \rangle}$ is open in A, and plainly $tA \le N$. Thus N is open. □

Proposition 4.2.6 *Let G be a finitely generated prosolvable group such that $[G, G]$ is closed. Then every subgroup N of finite index in G is open.*

Proof. Replacing N by its core N_G in G, we may assume that N is normal in G. We shall use induction on the index of N in G. By Corollary 4.2.4, G/N is a finite solvable group. If G/N is not of prime order, there exists some $H \triangleleft G$ with $N < H < G$. By induction H is open. According to Proposition 2.5.5, H is also a finitely generated profinite group. So, again by induction, N is open in H, and hence in G. Assume now that the order of G/N is p. Then $N \ge [G, G]$. Since $[G, G]$ is closed, we may assume that G is abelian. The result follows then from Proposition 4.2.5. □

Now we introduce the following terminology and notation. Given a natural number $\ell \ge 1$, we say that a finite group G is in the class $\mathcal{N}^\ell$, if G admits a normal series (i.e., $G_i \triangleleft G$ for all i)

$$G = G_0 \le G_1 \le \cdots \le G_{\ell-1} \le G_\ell = 1 \tag{1}$$

such that G_i/G_{i+1} is nilpotent ($i = 0, \ldots, \ell - 1$). Note that this condition on G is equivalent to simply assuming that the series (1) is subnormal (i.e., $G_{i+1} \triangleleft G_i$ for each i) rather than normal; indeed, if (1) is subnormal, replace each G_i in (1) by its core $\bigcap_{g\in G} G_i^g$ in G; then $\bigcap_{g\in G} G_i^g \triangleleft G$ and $G_{i-1}/\bigcap_{g\in G} G_i^g$ is a subgroup of $\prod_{g\in G} G_{i-1}/G_i^g$, which is nilpotent.

We claim that the class $\mathcal{N}^\ell$ is a formation of finite groups. Indeed, the class $\mathcal{N}^\ell$ is closed under taking quotient groups, because this is the case for the class of nilpotent groups. To see that $\mathcal{N}^\ell$ is closed under subdirect products, let G be a finite group, and assume that $N_i \triangleleft G$ with $G/N_i \in \mathcal{N}^\ell$ $(i = 1, 2)$; then $G/N_1 \cap N_2 \hookrightarrow G/N_1 \times G/N_2$. Since $\mathcal{N}^\ell$ is clearly closed under taking subgroups and finite direct products, we have that $G/N_1 \cap N_2 \in \mathcal{N}^\ell$.

The following are examples of classes of finite groups consisting of groups in $\mathcal{N}^\ell$, for some fixed ℓ:

- The class of all finite p-groups for a fixed prime p $(\ell = 1)$.
- The class of all finite nilpotent groups $(\ell = 1)$.
- The class of all finite supersolvable groups $(\ell = 2)$; this is because the commutator subgroup of a supersolvable group is nilpotent: see Hall [1959], Theorem 10.5.4.

Theorem 4.2.7 *Let G be a finitely generated profinite group such that there exists some fixed ℓ with $G/N \in \mathcal{N}^\ell$, whenever $N \triangleleft_o G$. Then every subgroup of G of finite index is open, i.e., G is strongly complete.*

The proof of this result will require first some preliminary lemmas.

Lemma 4.2.8 *Let $K \in \mathcal{N}^\ell$, with $\ell > 1$. Then K contains a smallest normal subgroup H such that $K/H \in \mathcal{N}^{\ell-1}$. Moreover*

(a) *H is nilpotent*; *and*
(b) *$[K, H] = H$.*

Proof. Certainly K contains normal subgroups L such that $K/L \in \mathcal{N}^{\ell-1}$, e.g., $K_{\ell-1}$; an easy induction shows that the intersection of two such normal subgroups of K has the same property; H is the intersection of all such normal subgroups of K. Part (a) is plain since $H \leq K_{\ell-1}$. Now, it is clear that $[K, H] \leq H$ and $[K, H] \triangleleft K$. Moreover, if

$$K = H_0 \geq H_1 \geq \cdots \geq H_{\ell-2} \geq H_{\ell-1} = H$$

is a normal series and each H_i/H_{i+1} is nilpotent $(i = 0, \ldots, \ell - 2)$, then

$$K = H_0 \geq [K, H_1] \geq \cdots \geq [K, H_{\ell-2}] \geq [K, H_{\ell-1}] = [K, H]$$

is a normal series; further $[K, H_i]/[K, H_{i+1}]$ is nilpotent since it is isomorphic to a subgroup of H_i/H_{i+1} $(i = 1, \ldots, \ell - 2)$, and $K/[K, H_1]$ is nilpotent since K/H_1 is nilpotent. Hence $K/[K, H] \in \mathcal{N}^{\ell-1}$. Thus, $[K, H] = H$ by the minimality of H. This proves (b). □

Proposition 4.2.9 *Let $K = \langle x_1, \ldots, x_r \rangle$ be a finitely generated abstract group.*

(a) *If A is an abelian normal subgroup of K, then every element of $[A, K]$ can be expressed in the form*

$$[a_1, x_1] \cdots [a_r, x_r]$$

$(a_1, \ldots, a_r \in A)$.

(b) *Assume that H is a nilpotent normal subgroup of K. Suppose that H is generated by $y_1, \dots, y_s$ as a normal subgroup, i.e., $H = \langle y_1, \dots, y_s \rangle^K$. Then every element of $[H, K]$ can be expressed in the form*

$$[h_1, x_1] \cdots [h_r, x_r][h'_1, y_1] \cdots [h'_s, y_s]$$

$(h_1, \dots, h_r, h'_1 \dots, h'_s \in H)$.

(c) *Assume that K is nilpotent. Then every element of $[K, K]$ can be expressed in the form*

$$[k_1, x_1] \cdots [k_r, x_r]$$

$(k_1, \dots, k_r \in K)$.

Proof. (a) Using the commutator identity

$$[ab, c] = [a, c]^b [b, c], \tag{2}$$

one deduces that $[A, x_i] = \{[a, x_i] \mid a \in A\}$ is a subgroup of A $(i = 1, \dots, r)$. Put $L = [A, x_1] \cdots [A, x_r]$. Since $a^{x_i} \equiv a \bmod(L)$ for each $a \in A$ $(i = 1, \dots, r)$, it follows that K centralizes A modulo L, i.e., $[A, K] \leq L$. On the other hand, it is obvious that $L \leq [A, K]$. Hence $[A, K] = L = [A, x_1] \cdots [A, x_r]$.

(b) We use induction on the nilpotency class c of H. If $c = 1$, H is abelian; then the result follows from part (a).

Assume now that $c > 1$. Consider the lower central series

$$H = \gamma_1(H) > \gamma_2(H) > \cdots > \gamma_{c-1}(H) > \gamma_c(H) > \gamma_{c+1}(H) = 1$$

of H. Put $B = \gamma_{c-1}(H)$ and $A = \gamma_c(H)$. Then, by definition, $[B, H] = A$ and $[A, H] = 1$. So, A is central in H. By part (a),

$$[A, K] = [A, x_1] \cdots [A, x_r],$$

since A abelian and normal in K.

By the centrality of A in H, one obtains from (2) that

$$[B, y_i] = \{[b, y_i] \mid b \in B\}$$

is a subgroup of $A = [B, K]$ $(i = 1, \dots, s)$. Put $J = [B, y_1] \cdots [B, y_s]$; then $J \leq A$.

We claim that $A = [A, K]J$, i.e., every element of A can be written in the form

$$[a_1, x_1] \cdots [a_r, x_r][b_1, y_1] \cdots [b_s, y_s],$$

for some $a_1, \dots, a_r \in A, b_1, \dots, b_s \in B$.

Plainly $[A, K]J \leq A$. Note that $[A, K]J \triangleleft K$, for $[J, K] \leq [A, K]$. Now, y_i centralizes $B/[A, K]J$, for each $i = 1, \dots, s$, since $[B, y_i] \leq J$; hence so does every conjugate y_i^g of y_i in K, for $B/[A, K]J$ is normal in $K/[A, K]J$. This means that H centralizes $B/[A, K]J$, i.e., $A = [H, B] \leq [A, K]J$. This proves the claim.

Let $u \in [H, K]$. By induction

$$u \equiv [h_1, x_1] \cdots [h_r, x_r][h'_1, y_1] \cdots [h'_s, y_s] \bmod (A),$$

where $h_1, \ldots, h_r, h'_1 \ldots, h'_s \in H$.

Therefore, by the above claim,

$$u = [h_1, x_1] \cdots [h_r, x_r][h'_1, y_1] \cdots [h'_s, y_s][a_1, x_1] \cdots [a_r, x_r][b_1, y_1] \cdots [b_s, y_s],$$

where $a_1, \ldots, a_r \in A, b_1, \ldots, b_s \in B$. Finally, since A is central in H we obtain

$$u = [h_1 a_1, x_1] \cdots [h_r a_r, x_r][h'_1 b_1, y_1] \cdots [h'_s b_s, y_s],$$

using the identity (2) again.

(c) We proceed by induction on the nilpotency class c of K. If $c = 1$, K is abelian and the result is trivial.

Suppose next that $c > 1$. Put $A = \gamma_c(K)$ and $B = \gamma_{c-1}(K)$. By the claim in part (b), every element of $a \in A$ can be written in the form $a = [b_1, x_1] \cdots [b_r, x_r]$, where $b_1, \ldots, b_r \in B$, since in this case A is central in K and we can take $\{y_1, \ldots, y_s\} = \{x_1, \ldots, x_r\}$.

Let $g \in [K, K]$. By induction,

$$g \equiv [k_1, x_1] \cdots [k_r, x_r] \bmod (A)$$

$(k_1 \ldots k_r \in K)$. Therefore,

$$g = [k_1, x_1] \cdots [k_r, x_r][b_1, x_1] \cdots [b_r, x_r],$$

for some $b_1, \ldots, b_r \in B$. Since $[b_1, x_1], \ldots, [b_r, x_r]$ are in the center of K, we can use (2) to get

$$g = [b_1 k_1, x_1] \cdots [b_r k_r, x_r]. \quad \square$$

Lemma 4.2.10 *Let $K = H \rtimes L$. If K can be generated by d elements, then there are d elements of H that generate it as a normal subgroup of K.*

Proof. Say $K = \langle k_1, \ldots, k_d \rangle$. Then $k_i = h_i x_i$, for some $h_i \in H, x_i \in L$ $(i = 1, \ldots, d)$. Consider the normal subgroup N of K generated by all the conjugates h_i^g $(i = 1, \ldots, d; g \in K)$. Clearly $N \leq H$; furthermore, $K = NL$ since NL contains each k_i. Thus $N = H$. In other words, $H = \langle h_1, \ldots, h_d \rangle^K$. $\square$

Finally, before we prove Theorem 4.2.7, we need a result on the splitting of some finite groups.

Lemma 4.2.11 *Let $K \in \mathcal{N}^\ell$ and let H be a minimal normal subgroup of K such that $K/H \in \mathcal{N}^{\ell-1}$. Assume further that H is abelian. Then there exists some subgroup L of K such that $K = H \rtimes L$.*

The proof of this result can be found in, for example, Doerk and Hawkes [1992], Theorem IV.5.18, where it is stated in the more general setting of "saturated formations". The class $\mathcal{N}^\ell$ is a formation. Moreover being "saturated" means that if L is a finite group and its Frattini quotient $L/\Phi(L)$ belongs to $\mathcal{N}^\ell$, then $L \in \mathcal{N}^\ell$; this is certainly so since the Frattini subgroup of a finite group is nilpotent (cf. Hall [1959], Theorem 10.4.2).

Proof of Theorem 4.2.7: According to Proposition 4.2.6, it suffices to show that $[G,G]$ is closed in G; and by Lemma 4.2.1, this would follow if we prove that there is an integer-valued function f such that if $K \in \mathcal{N}^\ell$ can be generated by k elements, then every element in $[K,K]$ is the product of $f(k)$ commutators. We shall show specifically that $f(k) = k + (\ell - 1)2k$.

We argue by induction on ℓ. If $\ell = 1$, then K is nilpotent and $f(k) = k$ by part (c) of Proposition 4.2.9.

Suppose now that $\ell > 1$ and that the result holds for $\ell - 1$. By Lemma 4.2.8, there exists a smallest normal subgroup H of K such that $K/H \in \mathcal{N}^{\ell-1}$; moreover H is nilpotent and $[H,K] = H$. It follows that the abelian group $H/[H,H]$ is the minimal normal subgroup of $K/[H,H]$ with quotient in $\mathcal{N}^{\ell-1}$. Then we infer from Lemma 4.2.11 that $K/[H,H] = H/[H,H] \rtimes L/[H,H]$ for some subgroup L such that $[H,H] \le L \le K$. By Lemma 4.2.10, there are elements $y_1, \ldots, y_k \in H$ such that $H = [H,H]\langle y_1, \ldots, y_k\rangle^K$. Since H is nilpotent, $[H,H] \le \Phi(H)$ (cf. Hall [1959], Theorem 10.4.3); hence $H = \langle y_1, \ldots, y_k\rangle^K$ (see Corollary 2.8.5). Then we can apply Proposition 4.2.9(b) to deduce that every element of $[H,K] = H$ is the product of $2k$ commutators. Let $g \in [K,K]$; by induction, the element $gH \in K/H$ is the product of $k + (\ell - 2)2k$ commutators of K/H; therefore $g = vh$, where v is the product of $k + (\ell - 2)2k$ commutators of K, and $h \in H$. Thus g is the product of $k + (\ell - 1)2k$ commutators of K, as claimed. □

Example 4.2.12 A nonstrongly complete group.

Let I be an infinite set, T a fixed nontrivial finite group and let $\mathcal{F}$ an ultrafilter on I containing the filter of all cofinite subsets of I (see, e.g., Bourbaki [1989], I, 6, 4). Consider the profinite group $G = \prod_I T$, the direct product of $|I|$ copies of T. Denote the elements of G by $\mathbf{g} = (g_i)$. We shall construct a nonopen subgroup H of index $|T|$ in G. Define H to be the collection of all elements $\mathbf{h} = (h_i)$ of G such that $\{i \in I \mid h_i = 1\} \in \mathcal{F}$. Plainly H is a proper normal subgroup of G. Moreover, it is dense in G since $\mathcal{F}$ contains all cofinite subsets of I. For $t \in T$, define $\mathbf{t} \in G$ as the element of G whose components t_i are all equal to t. To see that $[G : H] = |T|$, it suffices to show that every element $\mathbf{g} \in G$ is congruent to some such $\mathbf{t}$ modulo H. Now, fix $\mathbf{g} \in G$; for $t \in T$ define $I_t = \{i \in I \mid g_i = t\}$. Then

$$I = \bigcup_{t \in T} I_t.$$

Since $\mathcal{F}$ is an ultrafilter, $I_t \in \mathcal{F}$ for some $t \in T$. Therefore, $\mathbf{g}\mathbf{t}^{-1} \in H$, i.e., $\mathbf{g} \in G$ is congruent to $\mathbf{t}$ modulo H, as desired. Finally note that H is not open, since it is proper of finite index and it is dense.

For a profinite group G (not necessarily finitely generated) and a normal subgroup N of finite index, the property of N being open obviously implies the same property for its intersection with any Sylow subgroup of G; the following proposition establishes the converse of this.

Proposition 4.2.13 *Let G be a profinite group and let H be a normal subgroup of finite index. Then, H is open in G if and only if $H \cap P$ is open in P for every p-Sylow subgroup P of G.*

Proof. In one direction the result is evident. Conversely, let us assume that $H \cap P$ is open in P for each p-Sylow subgroup P of G. We must show that $H = \bar{H}$. Suppose on the contrary that $H \neq \bar{H}$; then there exists a element $x \in \bar{H} - H$ such that its image $\tilde{x}$ in the finite group $\bar{H}/H$ has order p for some prime p. We shall get a contradiction from the existence of such x. The induced homomorphism $\overline{\langle x \rangle} \longrightarrow \bar{H}/H$ is continuous since $\overline{\langle x \rangle}$ is strongly complete; hence, replacing x by x^{1_p} if necessary (see Section 4.1 for this notation), we may assume that x is a p-element. Let $\{x_i\}$ be a net in H converging to x. Note that since $\overline{\langle x_i \rangle}$ is strongly complete, $\overline{\langle x_i \rangle} \cap H$ is open in $\overline{\langle x_i \rangle}$; hence $\overline{\langle x_i \rangle} \leq H$. It follows then from Lemma 4.1.2 that $\{x_i^{1_p}\}$ is a net consisting of p-elements of H converging to x. We would reach the desired contradiction if we could prove the following claim: the set T of p-elements of H form a compact set. For then the limit x of any subnet of $\{x_i\}$ would have to be in H. Fix a p-Sylow subgroup P of G. To prove the claim, observe that T can be decomposed as

$$T = \bigcup_{g \in G} (H \cap P^g) = \bigcup_{g \in G} (H \cap P)^g,$$

since H is normal in G. On the other hand, T is the image of the continuous map

$$(H \cap P) \times G \longrightarrow H$$

given by $(r, g) \mapsto r^g$. Since, by hypothesis, $H \cap P$ is open in P, it is compact, and hence so is T. □

Exercise 4.2.14

(a) Let $G \longrightarrow H$ be a continuous epimorphism of profinite groups. Prove that if G is strongly complete, so is H.
(b) If the profinite group G is not strongly complete, then neither is any open subgroup of G.
(c) Let G be a strongly complete profinite group and let H be a profinite group. Show that every homomorphism $\varphi : G \longrightarrow H$ is continuous.

(d) Let

$$1 \longrightarrow G_1 \longrightarrow G \longrightarrow G_2 \longrightarrow 1$$

be an exact sequence of profinite groups. Show that if G_1 and G_2 are strongly complete, so is G.

4.3 Profinite Abelian Groups

In this section we study the structure of certain profinite abelian groups G. Namely those that are torsion-free or torsion or finitely generated. Our general approach consists of considering the Pontryagin dual group G^* of G; then use structure theorems for abstract abelian groups to describe this group; and finally dualize again to obtain the structure of $G \cong G^{**}$. Recall that a group G is called *torsion* if every element of G has finite order. If the orders of the elements of G are bounded, we say that G is *of finite exponent*; in that case, the least common multiple of all orders is called the *exponent* of G.

For the benefit of the reader we state next two structure results for abstract abelian groups that will be used in the sequel.

Theorem 4.3.1 (Fuchs [1970], Theorem 23.1; Hewitt and Ross [1963], Theorem A.14) *Let D be a divisible abstract abelian group. Then D is a direct sum of copies of* $\mathbf{Q}$ *and quasicyclic groups*:

$$D \cong \left[\bigoplus_{\mathfrak{n}} \mathbf{Q}\right] \oplus \left[\bigoplus_{p} \left(\bigoplus_{\mathfrak{m}(p)} C_{p^\infty}\right)\right],$$

where $\mathfrak{n}$ and $\mathfrak{m}(p)$ are cardinal numbers.

Before stating the next theorem we need the concept of purity. A subgroup B of an abelian group G is called *p-pure* (in G) if for whenever $x \in G$ and $x^{p^n} \in B$, then there exist some $y \in B$ such that $y^{p^n} = x^{p^n}$.

Theorem 4.3.2 (Fuchs [1970], Theorem 32.3; Hewitt and Ross [1963], Theorem A.24) *Let G be an abstract abelian group and let p be any prime number. Then G contains a subgroup B such that*

(a) *B is a direct sum of cyclic groups*;
(b) *B is p-pure*; *and*
(c) *G/B is p-divisible.*

Now we can classify torsion-free abelian profinite groups.

Theorem 4.3.3 *Let G be a torsion-free profinite abelian group. Then G is the direct product of copies of* $\mathbf{Z}_p$ *for all primes p*:

$$G \cong \prod_p \left(\prod_{\mathfrak{m}(p)} \mathbf{Z}_p\right),$$

where p ranges over all primes and each $\mathfrak{m}(p)$ is a cardinal number.

Proof. Consider the dual group G^* of G. By Theorems 2.9.6 and 2.9.12, G^* is a discrete abelian torsion divisible group. Hence, by Theorem 4.3.1,

$$G^* \cong \bigoplus_p \Big(\bigoplus_{\mathfrak{m}(p)} C_{p^\infty} \Big).$$

Thus, by Theorem 2.9.6, Example 2.9.5 and Lemma 2.9.4,

$$G \cong G^{**} \cong \prod_p \Big(\prod_{\mathfrak{m}(p)} (C_{p^\infty})^* \Big) \cong \prod_p \Big(\prod_{\mathfrak{m}(p)} \mathbf{Z}_p \Big). \quad \square$$

Theorem 4.3.4 *Let p be a fixed prime.*

(a) *Let G be a torsion-free pro-p abelian group. Then G is free (as a pro-p abelian group).*

(b) *Let G be a finitely generated pro-p abelian group. Then the torsion subgroup $tor(G)$ is finite, and*

$$G \cong F \oplus tor(G),$$

where F is a free pro-p abelian group of finite rank.

Proof. (a) This follows immediately from Theorem 4.3.3 and a result analogous to that in Example 3.3.8(c).

(b) Consider $tor(G)$ as an abstract group. By Theorem 4.3.2, G contains a subgroup B such that $tor(G)/B$ is divisible and B is a direct sum of cyclic p-groups. We claim that B is finite. Otherwise $B = \bigoplus_{i\in I} L_i$ where each L_i is a finite cyclic p-group and I is an infinite set. Now, for each finite subset J of I one has that $\bigoplus_{j\in J} L_j$ is a finite subgroup of G; hence $\bigoplus_{j\in J} L_j$ is closed in G. On the other hand, $d(\bigoplus_{j\in J} L_j) = |J|$; moreover $d(\bigoplus_{j\in J} L_j) \le d(G)$ since G is abelian. This is a contradiction since $d(G)$ is finite and since J can be chosen of arbitrarily large cardinality. This proves the claim. Therefore G/B is profinite. Since $tor(G)/B$ is divisible and torsion, it follows from Theorem 4.3.1 that either $tor(G)/B$ is trivial or $C_{p^\infty} \le G/B$. The second alternative is not possible since every subgroup of a profinite group is residually finite. Hence $tor(G) = B$ is finite.

Next observe that $G/tor(G)$ is a finitely generated torsion-free pro-p abelian group. By part (a), $G/tor(G)$ is a free pro-p abelian group of finite rank. Hence the short exact sequence

$$1 \longrightarrow tor(G) \longrightarrow G \xrightarrow{\varphi} G/tor(G) \longrightarrow 1$$

splits, that is, there exists a continuous homomorphism $\sigma : G/tor(G) \longrightarrow G$ such that $\varphi\sigma$ is the identity on $G/tor(G)$. Put $F = \sigma(G/tor(G))$. It follows that $G = F \oplus tor(G)$. $\square$

We remark that since abelian pro-p groups are in a natural way $\mathbf{Z}_p$-modules, one can deduce the theorem above from the general structure of modules over principal ideal domains.

Next we describe finitely generated profinite abelian groups. By Proposition 2.3.8 any such a group is the direct product of its pro-p components (p-Sylow subgroups). Hence its structure can be deduced immediately from the theorem above. We make it explicit in the following

Theorem 4.3.5 *Let G be a finitely generated profinite abelian group, with $d(G) = d$. Then, G is a direct sum of finitely many procyclic groups; more explicitly,*

$$G \cong \left[\bigoplus_p \left(\bigoplus_{m(p)} \mathbf{Z}_p\right)\right] \oplus \left[\bigoplus_p \left(\bigoplus_{i\in I_p} L_i(p)\right)\right],$$

where p ranges over all primes, each $L_i(p)$ is a finite cyclic p-group, each $m(p)$ is a natural number with $m(p) \le d$, and each I_p is a finite set with $|I_p| \le d$.

Proposition 4.3.6 *Let G be a finitely generated profinite abelian group, with $d(G) = d$. Let H be a closed subgroup of G. Then, H is also finitely generated and $d(H) \le d$.*

Proof. Say $G = \langle g_1, \dots, g_d\rangle$. Consider the chain of subgroups

$$1 \le G_1 \le G_2 \le \cdots \le G_d = G,$$

where G_i is the closed subgroup of G generated by $g_1, \dots, g_i$. Clearly G_{i+1}/G_i is a procyclic group $i = 1, \dots, d-1$. Set $H_i = H \cap G_i$. Then H_{i+1}/H_i a procyclic group since it is isomorphic to a subgroup of G_{i+1}/G_i (see Theorem 2.7.2). For each $i = 1, \dots, d-1$, choose $h_{i+1} \in H_{i+1}$ so that $h_{i+1}H_i$ generates H_{i+1}/H_i. Then clearly $H = \langle h_1, \dots, h_d\rangle$. Thus, $d(H) \le d$. □

We consider now profinite abelian torsion groups.

Lemma 4.3.7 *Let G be an abelian profinite torsion group. Then G is of finite exponent, i.e., there exists some integer $t \ge 1$ such that $g^t = 1$ for every $g \in G$.*

Proof. Since G is torsion, then $G = \bigcup_{n=1}^{\infty} G[n]$. Observe that each $G[n]$ is a closed subgroup of G. By Proposition 2.3.1, there is some m such that $G[m]$ has nonempty interior. Hence there exists an open normal subgroup U of G such that $U \subseteq G[n]$. Let $r = [G : U]$ and put $t = rm$. Then $g^t = 1$ for all $g \in G$. □

Theorem 4.3.8 *Let p be a fixed prime number and let G be a torsion pro-p abelian group. Then there exist a natural number e such that*

$$G \cong \prod_{i=1}^{e} \left(\prod_{\mathfrak{m}(i)} C_{p^i}\right),$$

where each $\mathfrak{m}(i)$ is a cardinal number.

Proof. By Lemma 4.3.7, there exists some natural number e such that $g^{p^e} = 1$ for all $g \in G$. Consider the dual group G^*. Then $p^e f = 0$ for all $f \in G^*$, i.e., G^* is of finite exponent. According to Theorem 4.3.2, G^* contains a subgroup B such that B is a direct sum of cyclic groups and G^*/B is divisible. It follows from Theorem 4.3.1 that a divisible group of finite exponent must be trivial. Hence $G^* = B$ is a direct sum of cyclic groups. Hence

$$G^* \cong \bigoplus_{i=1}^{e} \Big(\bigoplus_{\mathfrak{m}(i)} C_{p^i} \Big),$$

where each $\mathfrak{m}(i)$ is a cardinal number. The result follows now from Lemma 2.9.4. □

Corollary 4.3.9 *Let G be a torsion profinite abelian group. Then there exists a finite set of primes Π and a natural number e such that*

$$G \cong \prod_{p \in \Pi} \Big(\prod_{i=1}^{e} \Big(\prod_{\mathfrak{m}(i,p)} C_{p^i} \Big)\Big),$$

where each $\mathfrak{m}(i,p)$ is a cardinal number. In particular, G is of finite exponent.

Proof. Write G as a direct product $G = \prod_p G_p$ of its p-components. By Lemma 4.3.7, there is some positive integer $t \geq 1$ such that $g^t = 1$ for all $g \in G$. It follows that $G_p = 1$ if $p > t$. Then the result is now a consequence of Theorem 4.3.8. □

4.4 Automorphism Group of a Profinite Group

Let G be a profinite group and denote by $\mathrm{Aut}(G)$ the group of all continuous automorphisms of G. For a closed normal subgroup K of G, define

$$A_G(K) = \{\varphi \in \mathrm{Aut}(G) \mid \varphi(g)g^{-1} \in K \text{ for all } g \in G\}.$$

We make $\mathrm{Aut}(G)$ into a topological group by letting the sets $A_G(U)$ serve as a fundamental system of neighborhoods of 1, where U ranges over the set of all open normal subgroups of G (cf. Bourbaki [1989], III,1.2, Proposition 1). We term the corresponding topology the *congruence subgroup topology of* $\mathrm{Aut}(G)$. Note that $A_G(U)$ is the subgroup consisting of those automorphisms of G that leave U invariant and induce the trivial automorphism on G/U. Remark that

$$\bigcap_{U \triangleleft_o G} A_G(U) = \{\mathrm{id}\},$$

and therefore $\mathrm{Aut}(G)$ is totally disconnected (see Lemma 1.1.11). The next lemma shows that the congruence subgroup topology is the weakest topology on $\mathrm{Aut}(G)$ such that the holomorph $G \rtimes \mathrm{Aut}(G)$ is a topological group. [We refer the reader unfamiliar with actions of one group on another to Section 5.6, and in particular to Exercise 5.6.2.]

Lemma 4.4.1 *Let G be a profinite group.*

(a) *Consider* $\mathrm{Aut}(G)$ *as a topological group with the topology defined above. Then the natural action of* $\mathrm{Aut}(G)$ *on G is continuous*;
(b) *Suppose that* $\mathrm{Aut}(G)$ *is a topological group with respect to some topology and that the natural action of* $\mathrm{Aut}(G)$ *on G is continuous. Then $A_G(U)$ is an open subgroup of* $\mathrm{Aut}(G)$ *for every open normal subgroup U of G.*

Proof. (a) Define

$$\Psi : \mathrm{Aut}(G) \times G \longrightarrow G,$$

by $\Psi(\varphi, g) = \varphi(g)$. Choose $g \in G$, $U \leq_o G$. We need to show that the preimage $\Psi^{-1}(gU)$ of gU is open in $\mathrm{Aut}(G) \times G$. Pick $(\varphi_0, g_0) \in \Psi^{-1}(gU)$. It will suffice to find an open neighborhood of (φ_0, g_0) in $\mathrm{Aut}(G) \times G$ whose image under Ψ is contained in gU. Choose an open normal subgroup U_0 of G such that $U_0 \leq U$ and $\varphi_0(U_0) \leq U$ (this is possible since φ_0 is a continuous automorphism of G). Then $\varphi_0 A_G(U_0) \times g_0 U_0$ is clearly an open neighborhood of (φ_0, g_0) in $\mathrm{Aut}(G) \times G$. We show that $\Psi(\varphi_0 A_G(U_0) \times g_0 U_0) \subseteq gU$. Indeed, let $\varphi \in A_G(U_0)$ and $u \in U_0$. By the definition of $A_G(U_0)$, one has $\varphi(u) \in U_0$ and $\varphi(g_0) \in U_0 g_0 = g_0 U_0$. Thus

$$\Psi(\varphi_0\varphi, g_0 u) = (\varphi_0\varphi)(g_0 u) = (\varphi_0\varphi)(g_0)(\varphi_0\varphi)(u) \in \varphi_0(g_0)U = gU,$$

as required.

(b) Since $\mathrm{Aut}(G)$ acts continuously on G, the map

$$\Phi : \mathrm{Aut}(G) \times G \longrightarrow G,$$

$\Phi(\varphi, g) = \varphi(g)g^{-1}$ is continuous. Indeed, it is the composition

$$\mathrm{Aut}(G) \times G \longrightarrow G \times G \longrightarrow G$$

given by $(\varphi, g) \mapsto (\varphi(g), g) \mapsto \varphi(g)g^{-1}$, which is plainly continuous.

Let U be an open normal subgroup of G. Since $\Phi(\mathrm{id}, g) = 1$ for every $g \in G$, there exist an open neighborhood $A_{g,U}$ of the identity in $\mathrm{Aut}(G)$ and an open subgroup $V_{g,U}$ of G such that

$$\Phi(A_{g,U} \times gV_{g,U}) \subseteq U.$$

Clearly, $G = \bigcup_{g \in G} gV_{g,U}$. Since G is compact, there exist $g_1, \dots, g_n \in G$ such that $G = \bigcup_{i=1}^n g_i V_{g_i,U}$. Set $A = \bigcap_{i=1}^n A_{g_i,U}$. Then $\Phi(\varphi, g) \in U$ for all $\varphi \in A$ and $g \in G$. Thus, A is an open neighborhood of the identity in $\mathrm{Aut}(G)$ which is contained in $A_G(U)$. Hence, since $A_G(U)$ is a subgroup of $\mathrm{Aut}(G)$, we conclude that it is open. □

Theorem 4.4.2 *Let G be a profinite group. The congruence subgroup topology on* $\mathrm{Aut}(G)$ *defined above coincides with the compact-open topology of* $\mathrm{Aut}(G)$.

Proof. Let $U \triangleleft_o G$. We show first that $A_G(U)$ is open in the compact-open topology. Recall (see Section 2.9) that a subbase for the compact open-topology consists of the sets $B(K,V) = \{f \in \mathrm{Aut}(G) \mid f(K) \subseteq V\}$, where K runs through all the compact subsets of G and V runs through all the open subsets of G. Choose a transversal $g_1, \dots, g_n$ of U in G. Then

$$A_G(U) = \bigcap_{i=1}^{n} B(g_iU, g_iU),$$

so, $A_G(U)$ is open. Thus the compact-open topology is stronger than the congruence subgroup topology.

Conversely, let K be a compact subset of G, U an open normal subgroup of G and g an element of G. We need to show that $B(K, gU)$ is open in the congruence subgroup topology of $\mathrm{Aut}(G)$. Pick $\varphi_0 \in B(K, gU)$. It suffices to show that $A_G(U)\varphi_0 \subseteq B(K, gU)$. Indeed, for every $\varphi \in A_G(U)$ and every $k \in K$ one has

$$(\varphi\varphi_0)(k) \in \varphi(gU) \subseteq gU. \quad \square$$

Next we give conditions on G for the group $\mathrm{Aut}(G)$ to be profinite.

Proposition 4.4.3 *Assume that a profinite group G admits a fundamental system $\mathcal{U}_c$ of open neighborhoods of 1 such that each $U \in \mathcal{U}_c$ is a characteristic subgroup of G. Then $\mathrm{Aut}(G)$ is a profinite group.*

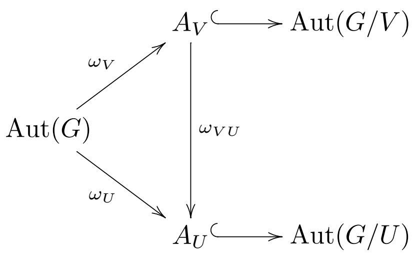
Proof. Let $U \in \mathcal{U}_c$. Then $A_G(U)$ is the kernel of the natural homomorphism

$$\omega_U : \mathrm{Aut}(G) \longrightarrow \mathrm{Aut}(G/U),$$

and ω_U is continuous for each $U \in \mathcal{U}_c$. Define $A_U = \omega_U(\mathrm{Aut}(G))$. For $\varphi \in \mathrm{Aut}(G)$, put $\varphi_U = \omega_U(\varphi)$ $(U \in \mathcal{U}_c)$. For $V \le U$ $(U, v \in \mathcal{U}_c)$, the map

$$\omega_{VU} : A_V \longrightarrow A_U$$

given by $\omega_{VU}(\varphi_V) = \varphi_U$, is a well-defined homomorphism; furthermore by definition one has a commutative diagram



Hence the family of continuous homomorphisms $\{\omega_U\}_{U \in \mathcal{U}_c}$ induces a continuous epimorphism (see Corollary 1.1.6)

$$\omega : \mathrm{Aut}(G) \longrightarrow \varprojlim_{U \in \mathcal{U}_c} A_U$$

Observe that ω is an injection since $\mathrm{Ker}(\omega) = \bigcap_{U \in \mathcal{U}_c} A_G(U) = \{\mathrm{id}\}$. Therefore

$$\mathrm{Aut}(G) = \varprojlim_{U \in \mathcal{U}_c} A_U$$

is a profinite group. □

Combining the proposition above with Proposition 2.5.1, we get

Corollary 4.4.4 *Let G be a finitely generated profinite group. Then* $\mathrm{Aut}(G)$ *is a profinite group.*

The following exercise indicates how to construct infinitely generated profinite groups satisfying the hypotheses of Proposition 4.4.3.

Exercise 4.4.5 Let $\mathcal{S}$ be the set of all (nonisomorphic) finite simple groups. For each $S \in \mathcal{S}$, let P_S be a direct product of finitely many copies of S. Define

$$G = \prod_{S \in \mathcal{S}} P_S.$$

Prove that G is not finitely generated, but it has only finitely many open subgroups of any given index n. Deduce that $\mathrm{Aut}(G)$ is a profinite group.

Next we present an example of a profinite group G to show that $\mathrm{Aut}(G)$ need not be profinite.

Example 4.4.6 Let C_2 be the cyclic group of order 2 and let

$$G = \prod_I G_i$$

be a direct product indexed by an infinite set I such that $G_i \cong C_2$ for all $i \in I$. Let U be a subgroup of G of index 2 containing all but one of the direct factors. Denote by c_i the generator of G_i $(i \in I)$, and let $i_0 \in I$ be such that $c_{i_0} \notin U$. We shall prove that $\mathrm{Aut}(G)$, with the congruence subgroup topology, is not compact. To see this it is enough to show that the open subgroup $A_G(U)$ has infinite index in $\mathrm{Aut}(G)$. For $i \in I$, $i \neq i_0$, denote by f_i the automorphism of G that permutes c_{i_0} and c_i and fixes the rest of the c_j $(j \in I)$. Then for any pair $i \neq j$ in $I - \{i_o\}$, one has $f_i^{-1} f_j(c_i) = c_{i_0} \notin U$, i.e., $f_i^{-1} f_j \notin A_G(U)$. This shows that the f_i $(i_o \neq i \in I)$ lie in different cosets of $A_G(U)$. Hence $A_G(U)$ has infinite index in $\mathrm{Aut}(G)$. Thus $\mathrm{Aut}(G)$ is not compact and therefore not profinite.

Next we calculate the automorphism groups of $\mathbf{Z}_p$ and $\widehat{\mathbf{Z}}$.

Theorem 4.4.7 *Let p be a prime number. Then*

(a) $\mathrm{Aut}(\mathbf{Z}_p) \cong \mathbf{Z}_p \times C_{p-1}$, *if* $p \neq 2$; *and*
(b) $\mathrm{Aut}(\mathbf{Z}_2) \cong \mathbf{Z}_2 \times C_2$.

Proof. By Proposition 4.4.3,

$$\mathrm{Aut}(\mathbf{Z}_p) \cong \varprojlim_n \mathrm{Aut}(\mathbf{Z}/p^n\mathbf{Z}).$$

Denote by R_n the ring $\mathbf{Z}/p^n\mathbf{Z}$ of integers modulo p^n $(n = 1, 2, \ldots)$. One easily checks that the automorphism group of the additive cyclic group $\mathbf{Z}/p^n\mathbf{Z}$ can be identified with the multiplicative group $R_n^\times$ of units of the ring R_n. Recall that an integer represents a unit in R_n if and only if it is prime to p. Therefore, $|R_n| = p^{n-1}(p-1)$.

For $m \geq n$, let $\varphi_{m,n} : R_m \longrightarrow R_n$ be the canonical epimorphism. Clearly

$$\varphi_{m,n}(R_m^\times) = R_n^\times.$$

Next we prove the following *Claim*:

$$R_n^\times \cong \begin{cases} C_{p^{n-1}} \times C_{p-1}, & \text{if } p \neq 2; \\ C_{2^{n-2}} \times C_2, & \text{if } p = 2 \text{ and } n \geq 3; \\ C_2, & \text{if } p = 2 \text{ and } n = 2; \\ 1, & \text{if } p = 2 \text{ and } n = 1. \end{cases} \quad \text{and}$$

Before proving the claim, note that the theorem follows from the claim if $p \neq 2$. For $p = 2$, the theorem will also follow once we describe more precisely the two factors in $R_n^\times$ corresponding to the decomposition $C_{2^{n-2}} \times C_2$ $(n \geq 3)$.

Assume that α is an integer and let i be a natural number such that $\alpha^i \equiv 1 \pmod{p^n}$. Then $\alpha^i \equiv 1 \pmod{p}$; so $p - 1 \mid i$. Therefore the order of α in $R_n^\times$ is a multiple of $p-1$. Replacing α by one of its powers, we deduce that there is an element of order $p-1$ in $R_n^\times$; we denote this element still by α.

If $x \in \mathbf{Z}$ satisfies $x \equiv 1 + rp^t \pmod{p^{t+2}}$ and $t \geq 1$, one can use the binomial expansion to get

$$x^p \equiv 1 + rp^{t+1} + \frac{p(p-1)}{2} r^2 p^{2t} \pmod{p^{t+2}}. \tag{3}$$

If follows from this that if $x \equiv 1 \pmod{p^t}$, then $x^p \equiv 1 \pmod{p^{t+1}}$. If one assumes that either $p \neq 2$ or $t > 1$, then (3) implies that if $x \equiv 1 \pmod{p^t}$ but $x \not\equiv 1 \pmod{p^{t+1}}$, then $x^p \not\equiv 1 \pmod{p^{t+2}}$.

We distinguish two cases. Assume first that $p \neq 2$. Then the above remarks together with an induction argument show that the element $\beta = 1 + p$ has order p^{n-1} in the group $R_n^\times$. Since the orders of α and β are relatively prime, we deduce that

$$R_n^\times = \langle \alpha\beta \rangle = \langle \alpha \rangle \times \langle \beta \rangle \cong C_{p^{n-1}} \times C_{p-1},$$

as desired.

Assume now that $p = 2$. If $n = 1$, then clearly $R_1^\times = (\mathbf{Z}/2\mathbf{Z})^\times \cong C_1$, the trivial group; and if $n = 2$, then clearly $R_2^\times = (\mathbf{Z}/2^2\mathbf{Z})^\times \cong C_2$. Suppose $n \geq 3$. Then it follows from the argument indicated above using (3), that 5 has order 2^{n-2} in $R_n^\times = (\mathbf{Z}/2^n\mathbf{Z})^\times$. On the other hand -1 is not in the subgroup $L(n,5) = \langle 5 \rangle$ of $R_n^\times$ generated by 5; this is the case because otherwise

$$-1 \equiv 1 \pmod 4$$

(since $5 \equiv 1 \pmod 4$ and $R_2^\times = (\mathbf{Z}/2^2\mathbf{Z})^\times$ is a quotient of $R_n^\times = (\mathbf{Z}/2^n\mathbf{Z})^\times$), a contradiction. Consider the subgroup $L(n,-1) = \langle -1 \rangle$ of $R_n^\times$ generated by -1. It follows that

$$R_n^\times = (\mathbf{Z}/2^n\mathbf{Z})^\times = L(n,5) \times L(n,-1) \cong C_{2^{n-2}} \times C_2,$$

as asserted. This ends the proof of the claim.

To finish the proof of the theorem in the remaining case $p = 2$, observe that (for $m \geq n \geq 3$), one has

$$\varphi_{m,n}(L(m,5)) = L(n,5) \quad \text{and} \quad \varphi_{m,n}(L(m,-1)) = L(n,-1).$$

Thus

$$\varprojlim_n \operatorname{Aut}(\mathbf{Z}/2^n\mathbf{Z}) = \varprojlim_n (L(n,5) \times L(n,-1)) \cong \mathbf{Z}_2 \times C_2. \quad \square$$

Corollary 4.4.8

$$\operatorname{Aut}(\widehat{\mathbf{Z}}) \cong \mathbf{Z}_2 \times C_2 \times \prod_p (\mathbf{Z}_p \times C_{p-1}).$$

In particular, $\operatorname{Aut}(\widehat{\mathbf{Z}})$ *is infinitely generated.*

It is well known that the automorphism group of a free abstract group of finite rank is finitely generated (cf. Magnus, Karras and Solitar [1966], Theorem 3.5.N1). The corollary above shows that the corresponding result for profinite groups fails even for cyclic groups. Next we state a result of Roman'kov [1993] which shows that it also fails for pro-p groups.

Theorem 4.4.9 *Let F be a free pro-p group of rank $m \geq 2$. Then* $\operatorname{Aut}(F)$ *is an infinitely generated profinite group.*

4.5 Automorphism Group of a Free Pro-p Group

Let F be a free pro-p group of finite rank. In this section we study the group of automorphisms $\operatorname{Aut}(F)$ of F. In the previous section we have already described this automorphism group when F has rank 1.

We start with some definitions and results valid for profinite groups in general. Let G be a profinite group and let $\gamma_n(G)$ $(n = 1, 2, 3, \dots)$ denote the (closure) of the n-th term of its lower central series (see Exercise 2.3.17). Define

$$A_n(G) = \operatorname{Ker}\big(\operatorname{Aut}(G) \longrightarrow \operatorname{Aut}(G/\gamma_{n+1}(G))\big).$$

Thus we have a series of normal subgroups

$$\cdots \triangleleft A_2(G) \triangleleft A_1(G) \triangleleft \operatorname{Aut}(G).$$

Our first aim is to establish the following

Proposition 4.5.1 *Let G be a profinite group. Then, G is pronilpotent if and only if $A_1(G)$ is pronilpotent.*

Before proving this result, we need two technical lemmas. They are valid for general groups, but we shall state them only for profinite groups for convenience in our exposition.

Lemma 4.5.2 *Let G be a profinite group and let K, L, H be closed subgroups of G. Put*

$$U = \overline{[[K,L],H]}, \qquad V = \overline{[[L,H],K]} \quad \text{and} \quad W = \overline{[[H,K],L]}.$$

Then, any normal subgroup N of G containing U and V, contains W as well.

Proof. We use the following Witt-Hall identity, which can be easily checked,

$$[[x,y^{-1}],z]^y[[y,z^{-1}],x]^z[[z,x^{-1}],y]^x = 1.$$

Choose $x \in H$, $y \in K$, $z \in L$. Then the three factors on the left hand side of the above identity belong to W^y, U^z, and V^x, respectively. Since $U^z \leq N$, $V^x \leq N$, one deduces that $[[x,y^{-1}],z] \in N$ for all $x \in H$, $y \in K$, $z \in L$. The commutators $[x,y^{-1}]$ generate $\overline{[H,K]}$ topologically. Consequently, every element of L commutes modulo N with every element of $\overline{[H,K]}$. In other words, $W = \overline{[[H,K],L]}$ is also in N, as required. □

Lemma 4.5.3 *Let G be a profinite group. For every pair of natural numbers i, j, one has (we think of G and $\operatorname{Aut}(G)$ as subgroups of $G \rtimes \operatorname{Aut}(G)$)*

(a) $\overline{[\gamma_i(G), A_j(G)]} \leq \gamma_{i+j}(G)$;

(b) $\overline{[A_i(G), A_j(G)]} \leq A_{i+j}(G)$.

Proof. (a) We use induction on i. First note that by definition of $A_n(G)$ one has $\overline{[G, A_j(G)]} \leq \gamma_{j+1}(G)$; so, (a) holds for $i = 1$. Suppose now that $\overline{[\gamma_i(G), A_j(G)]} \leq \gamma_{i+j}(G)$. By the induction hypothesis one has

$$\overline{[\gamma_i(G),[G,A_j(G)]]} \leq \overline{[\gamma_i(G),\gamma_{j+1}(G)]} \leq \gamma_{i+j+1}(G)$$

and
$$\overline{[[A_j(G),\gamma_i(G)],G]} \le \overline{[\gamma_{i+j}(G),G]} = \gamma_{i+j+1}(G).$$
Hence, by Lemma 4.5.2,
$$\overline{[[G,\gamma_i(G)],A_j(G)]} = \overline{[\gamma_{i+1}(G),A_j(G)]} \le \gamma_{i+j+1}(G),$$
as required.

(b) By (a) one has
$$\overline{[A_j(G),[G,A_i(G)]]} \le \overline{[\gamma_{i+1}(G),A_j(G)]} \le \gamma_{i+j+1}(G).$$
Therefore, using Lemma 4.5.2 we deduce
$$\overline{[[A_i(G),A_j(G)],G]} \le \gamma_{i+j+1}(G).$$
Hence
$$\overline{[A_i(G),A_j(G)]} \le A_{i+j}(G),$$
by definition of $A_{i+j}(G)$. □

Proof of Proposition 4.5.1. Let $Z(G)$ denote the center of G. We think of $G/Z(G)$ as a group of inner automorphisms of G. Since inner automorphisms act trivially on the commutator quotient, we have that $G/Z(G)$ is a subgroup of $A_1(G)$. If $A_1(G)$ is pronilpotent, so is $G/Z(G)$, and hence so is G.

Conversely, if G is pronilpotent then $\bigcap_{n=1}^{\infty}\gamma_n(G)=1$ (see Exercise 2.3.17). So $\bigcap_{n=1}^{\infty}A_n(G)=1$. We claim that $A_n(G)$ contains $\gamma_n(A_1(G))$. We use induction on n. By Lemma 4.5.3(b), $\overline{[A_1(G),A_1(G)]} \le A_2(G)$. Assuming that $\gamma_{n-1}(A_1(G)) \le A_{n-1}(G)$, we deduce from Lemma 4.5.3(b) that
$$\gamma_n(A_1(G)) \le \overline{[A_{n-1}(G),A_1(G)]} \le A_n(G),$$
proving the claim. This implies that $\bigcap_{n=1}^{\infty}\gamma_n(A_1)=1$. Hence A_1 is pronilpotent. □

Proposition 4.5.4 *Let $\mathcal{C}$ be a formation of finite groups and let $F=F(n)$ be a free pro-$\mathcal{C}$ group of finite rank n.*

(a) *Suppose that M and N are closed normal subgroups of F such that F/M and F/N are isomorphic. Then every continuous isomorphism $\beta : F/M \longrightarrow F/N$ is induced by a corresponding continuous automorphism α of F. In other words the diagram*
$$\begin{array}{ccc} F & \xrightarrow[\alpha]{\cong} & F \\ \varphi\downarrow & & \downarrow\psi \\ F/M & \xrightarrow[\beta]{\cong} & F/N \end{array}$$
commutes, where φ and ψ are the canonical epimorphisms.

(b) *Let K be a characteristic subgroup of F. Then the natural homomorphism*

$$\omega_K : \mathrm{Aut}(F) \longrightarrow \mathrm{Aut}(F/K)$$

is an epimorphism.

Proof. Part (b) follows from part (a). To prove part (a), choose a basis $X = \{x_1, \dots, x_n\}$ of F. For $i = 1, 2, \dots, n$, set $z_i = (\beta\varphi)(x_i)$. Then F/N is generated by $z_1, \dots, z_n$. Since $n = d(F)$, by Proposition 2.5.4, there exist elements $y_1, \dots, y_n$ in F such that $F = \overline{\langle y_1, \dots, y_n \rangle}$ and $\psi(y_i) = z_i$ $(i = 1, 2, \dots, n)$. Define a continuous epimorphism $\alpha : F \longrightarrow F$ by $\alpha(x_i) = y_i$ $(i = 1, 2, \dots, n)$. By the Hopfian property of F (see Proposition 2.5.2), we deduce that α is an automorphism. Clearly $\psi\alpha = \beta\varphi$. □

Lemma 4.5.5 *Let G be a finitely generated pro-p group. Then the kernel $K_1(G)$ of the natural epimorphism*

$$\mathrm{Aut}(G) \longrightarrow \mathrm{Aut}(G/\Phi(G))$$

is a pro-p group. In particular $\mathrm{Aut}(G)$ *has an open pro-p subgroup.*

Proof. The result is well-known if G is finite (see Hall [1959], Theorem 12.2.2). By Proposition 2.8.13, the terms $\Phi_n(G)$ of the Frattini series form a fundamental system of neighborhoods of 1 in the group G. It follows from Corollary 4.4.4, Corollary 2.8.3 and the exactness of inverse limits (see Proposition 2.2.4) that

$$K_1(G) = \varprojlim_n K_1(G/\Phi_n(G)).$$

Thus the lemma follows from the corresponding result for finite groups mentioned above. □

In the following theorem we collect some of the results obtained above in the case of the automorphism group of a free pro-p group, and we obtain some new information.

Theorem 4.5.6 *Let F be a free pro-p group of finite rank $m \geq 2$. Let $A_n(F)$ be the kernel of the natural epimorphism*

$$\mathrm{Aut}(F) \longrightarrow \mathrm{Aut}(F/\gamma_{n+1}(F)) \quad (n = 1, 2, \dots).$$

Then

(a) *Each $A_n(F)$ is a normal pro-p subgroup of $Aut(F)$ and*

$$\cdots \lhd A_2(F) \lhd A_1(F) \lhd \mathrm{Aut}(F).$$

(b) $\bigcap_{n=1}^{\infty} A_n(F) = \{1\}$;
(c) $\mathrm{Aut}(F)/A_1(F)$ *is isomorphic to* $GL_m(\mathbf{Z}_p)$; *and*

(d)

$$A_{n-1}(F)/A_n(F)$$

is a free abelian pro-p group of rank $d(F)d(\gamma_n(F)/\gamma_{n+1}(F))$.

Proof. The fact that $\mathrm{Aut}(F) \longrightarrow \mathrm{Aut}(F/\gamma_n(F))$ is an epimorphism is the content of Proposition 4.5.4. Part (a) follows from the definition of $A_n(F)$ and Lemma 4.5.5, since (using the notation in that proposition) $A_1(F) \leq K_1(F)$. Part (b) follows from the equality $\bigcap_{i=1}^{\infty} \gamma_n(F) = 1$ (see Exercise 2.3.17). Part (c) is obvious.

It remains to prove (d). By the definition of $A_n(F)$, we may identify $\mathrm{Aut}(F)/A_n(F)$ with $\mathrm{Aut}(F/\gamma_{n+1}(F))$, and $A_{n-1}(F)/A_n(F)$ with the set of those automorphisms of $F/\gamma_{n+1}(F)$ which induce the identity on $F/\gamma_n(F)$. Define

$$\Psi : A_{n-1}(F)/A_n(F) \longrightarrow \mathrm{Hom}(F/\gamma_{n+1}(F), \gamma_n(F)/\gamma_{n+1}(F))$$

by $\Psi(\alpha)(z) = \alpha(z)z^{-1}$ for all $\alpha \in A_{n-1}(F)/A_n(F)$, $z \in F/\gamma_{n+1}(F)$ (it is straightforward to check that $\Psi(\alpha) \in \mathrm{Hom}(F/\gamma_{n+1}(F), \gamma_n(F)/\gamma_{n+1}(F))$). We first show that Ψ is an (algebraic) isomorphism.

To show that Ψ is a homomorphism pick $\alpha, \beta \in A_{n-1}(F)/A_n(F)$. Then for any $z \in F/\gamma_{n+1}(F)$ one has

$$\Psi(\alpha\beta)(z) = \alpha\beta(z)z^{-1} = \alpha(\beta(z)z^{-1})\alpha(z)z^{-1} = \alpha(z)z^{-1}\beta(z)z^{-1},$$

where the last equality follows from the fact that $\beta(z)z^{-1} \in \gamma_n(F)/\gamma_{n+1}(F)$ and hence is centralized by α. On the other hand,

$$\Psi(\alpha)\Psi(\beta)(z) = \alpha(z)z^{-1}\beta(z)z^{-1},$$

and so the equality $\Psi(\alpha\beta) = \Psi(\alpha)\Psi(\beta)$ is proved.

Now, $\Psi(\alpha(z)) = 0$ for all $z \in F/\gamma_{n+1}(F)$ if and only if $\alpha(z)z^{-1} = 0$ for all z; and this is equivalent to $\alpha = \mathrm{id}$, which proves injectivity.

To prove surjectivity choose

$$\tau \in \mathrm{Hom}(F/\gamma_{n+1}(F), \gamma_n(F)/\gamma_{n+1}(F)),$$

and define $\alpha_\tau : F/\gamma_{n+1}(F) \longrightarrow F/\gamma_{n+1}(F)$ by $\alpha_\tau(z) = \tau(z)z$ for all $z \in F/\gamma_{n+1}(F)$. Since $\tau(z) \in \gamma_n(F)/\gamma_{n+1}(F)$, α_τ is a homomorphism and since $\tau(\overline{[F,F]})$ is trivial, it is an automorphism of $F/\gamma_{n+1}(F)$ which induces the identity automorphism modulo $\gamma_n(F)$, i.e., $\alpha_\tau \in A_{n-1}(F)/A_n(F)$. Clearly $\Psi(\alpha_\tau) = \tau$.

Let X be a basis for F. Since $F/\gamma_{n+1}(F)$ is a free nilpotent pro-p group of class n, the group $\mathrm{Hom}(F/\gamma_{n+1}(F), \gamma_n(F)/\gamma_{n+1}(F))$ is isomorphic to a direct product

$$\prod_{|X|}(\gamma_n(F)/\gamma_{n+1}(F))$$

of $|X|$ copies of $\gamma_n(F)/\gamma_{n+1}(F)$. Let

$$\Phi : A_{n-1}(F)/A_n(F) \longrightarrow \prod_{|X|}(\gamma_n(F)/\gamma_{n+1}(F))$$

be a composition of this isomorphism with Ψ. We prove that the isomorphism Φ is topological.

Let U be an open normal subgroup of $F/\gamma_{n+1}(F)$ which is contained in $\gamma_n(F)/\gamma_{n+1}(F)$. Then

$$\begin{aligned}\Phi^{-1}\left(\prod_{|X|} U\right) &= \{\alpha \in A_{n-1}(F)/A_n(F) \mid \alpha(z)z^{-1} \in U \text{ for all } z \in F/\gamma_{n+1}(F)\} \\ &= A_U(F)/\gamma_{n+1}(F)\end{aligned}$$

is open in $\mathrm{Aut}(F/\gamma_{n+1}(F))$ and therefore so is in $A_{n-1}(F)/A_n(F)$. □

4.6 Profinite Frobenius Groups

The aim of this section is to characterize those profinite groups that can be written as surjective inverse limits of finite Frobenius groups. Finite Frobenius groups can be described in terms of many equivalent properties; we mention some of these descriptions in Theorem 4.6.1. Not all those properties remain equivalent for general profinite groups (see Example 4.6.2).

A closed subgroup H of a profinite group G is called *isolated* if $1 < H < G$ and whenever $g \in G - H$, then $H \cap H^g = 1$.

Let H and K be groups. Assume that H acts on K, and denote the action of $h \in H$ on $k \in K$ by k^h. We say that this action is *fixed-point-free* if $k^h \neq k$ whenever $h, k \neq 1$ ($h \in H$ $k \in K$).

We remark that the actions involving (infinite) profinite groups that we consider in this section are always by conjugation inside profinite groups; hence such actions are automatically continuous. For a more general approach to continuous actions see Section 5.6.

A profinite group G is called *Frobenius* if it contains a closed isolated Hall subgroup H. If G is finite, the condition on H being Hall is redundant. Next we recall some properties of Frobenius groups in the case that G is finite. See, for example, Huppert [1967], Section V.8, for proof of the following result where we collect some of the principal properties of finite Frobenius groups.

Theorem 4.6.1 *Let G be a finite group.*

(a) *G is a Frobenius group if and only if G has an isolated subgroup H; an isolated subgroup of a finite group is automatically a Hall subgroup; an isolated subgroup of G is called a Frobenius complement.*

(b) *G is a Frobenius group if and only if there exists a proper nontrivial normal subgroup K of G such that for each* $k \in K$, $k \neq 1$, *one has* $\mathrm{C}_G(k) \leq K$ ($\mathrm{C}_G(k)$ *is the centralizer of k in G*); *such K is called a Frobenius kernel of G*; *there is only one Frobenius kernel in a finite Frobenius group*; *any complement H of K in G is an isolated subgroup.*

(c) *G is a Frobenius group if and only if there exists a proper nontrivial subgroup H of G such that the set* $K = [G - (\bigcup_{g \in G} H^g)] \cup \{1\}$ *is a subgroup of G*; *then K is the Frobenius kernel of G and H a Frobenius complement.*

(d) *G is a Frobenius group if and only if G can be expressed as a nontrivial semidirect product* $G = K \rtimes H$ *and the action of H on K by conjugation is fixed-point-free*; *then K is the Frobenius kernel of G and H a Frobenius complement.*

(e) *Let* $G = K \rtimes H$ *be a finite Frobenius group with Frobenius kernel K. Let* $L \lhd G$; *then either* $L \leq K$ *or* $L \geq K$; *if* $L < K$, *then* G/L *is Frobenius with Frobenius kernel* K/L.

(f) *Let* $G = K \rtimes H$ *be a finite Frobenius group with Frobenius kernel K and Frobenius complement H. Then*
   (1) *K is nilpotent*;
   (2) *Let p be a prime number. If* $p \neq 2$, *then a p-Sylow subgroup of H is cyclic. The* 2*-Sylow subgroups of H are either cyclic or generalized quaternion.*

Example 4.6.2 (1) Define the *infinite dihedral pro*-2 *group* to be the pro-2 group D with presentation

$$D = \langle x, y \mid y^2 = 1, yxy^{-1} = x^{-1} \rangle,$$

i.e., $D = F/R$, where F is a free pro-2 group on a basis x, y, and R is the smallest closed normal subgroup of F containing the elements y^2 and $yxy^{-1}x$. Denote by a and b the images in D of x and y respectively. Then b has order 2, $\overline{\langle a \rangle} \cong \mathbf{Z}_2$ and $G = \overline{\langle a \rangle} \rtimes \langle b \rangle$. Note that $\langle b \rangle$ is isolated in G, but it is not a Hall subgroup.

(2) Let $p < q$ be two distinct primes and assume that $p \mid q - 1$. By Corollary 4.4.4, there is an embedding of C_p into $\mathrm{Aut}(\mathbf{Z}_q)$. This corresponds to an action of $H = C_p$ on $K = \mathbf{Z}_q$ given by multiplication in $\mathbf{Z}_q$ by a unit of the ring $\mathbf{Z}_q$; therefore this action is fixed-point-free. Construct the corresponding semidirect product $G = K \rtimes H$ (see Exercise 5.6.2). This implies (see Lemma 4.6.3 below) that, H is isolated, and so G is Frobenius.

Lemma 4.6.3 *Let* $G = K \rtimes H$ *be a semidirect product of K by H such that* $1 < H < G$. *Then H is isolated if and only if H acts fixed-point-free on K* (*by conjugation*).

Proof. Let $g \in G$. Then there exists some $k \in K$ such that $H^g = H^k$, since $G = KH$. Let $1 \neq k \in K$; then $H^k \cap H \neq 1$ if and only if $h^k = h$ for some

$1 \neq h \in H$ (because K is normal and $H \cap K = 1$) if and only if $k^h = k$ for some $1 \neq h \in H$. Thus the result follows. □

Lemma 4.6.4 *Let G be a profinite group and let H be a closed isolated Hall subgroup of G. Then*

(a) *H is finite*;
(b) *The Sylow subgroups of H are either cyclic or generalized quaternion groups. In particular, a p-Sylow subgroup of H contains a unique subgroup of order p.*

Proof. (a) Let q be a prime number such that $q \mid [G : H]$. Then there exists some $U \triangleleft_o G$ with $q \mid [G : UH]$; so, q divides $[G : U]$. Assume that H is infinite. Then $H \cap U \neq 1$. Therefore, there exists a prime number p and a p-Sylow subgroup P of H such that $P_1 = P \cap U \neq 1$. Note that P_1 is a p-Sylow subgroup of U, since P is also a p-Sylow subgroup of G. By the Frattini argument (see Exercise 2.3.13), $G = \mathrm{N}_G(P_1)U$. Therefore,

$$G/U \cong \mathrm{N}_G(P_1)/U \cap \mathrm{N}_G(P_1);$$

hence q divides the order of $\mathrm{N}_G(P_1)$. Let Q be a q-Sylow subgroup of $\mathrm{N}_G(P_1)$, and choose $1 \neq y \in Q$; observe that $y \notin H$. Then

$$P_1 = P_1 \cap P_1^y \leq H \cap H^y = 1,$$

a contradiction. Thus H is finite.

(b) These are well-known properties of isolated subgroups in finite groups (see Theorem 4.6.1). So, it suffices to show that H appears as an isolated subgroup of a finite group. Assume that G is infinite. Since H is finite, there exists some open normal subgroup U of G with $U \cap H = 1$. Choose an open normal subgroup W of G such that $W < U$. Consider the profinite group $UH = U \rtimes H$. By Lemma 4.6.3, H acts fixed-point-free on U. It follows from Proposition 2.3.16, that H acts fixed-point-free on U/W. Hence $U/W \rtimes H$ is a finite Frobenius group where H is isolated. □

Lemma 4.6.5 *Let G be a profinite group and let H be a closed isolated Hall subgroup of G.*

(a) *H has a unique closed normal complement K, i.e., a closed normal subgroup K of G such that $G = KH$ and $K \cap H = 1$, so that $G = K \rtimes H$;*
(b) *Let $\mathcal{V}$ be the collection of all open normal subgroups V of G such that $V < K$. Then, $G/V = (K/V) \rtimes (HV/V)$ is a finite Frobenius group with isolated subgroup HV/V for each $V \in \mathcal{V}$, and*

$$G = \varprojlim_{V \in \mathcal{V}} \left[(K/V) \rtimes (HV/V)\right].$$

Proof. By Lemma 4.6.4, H is finite. We first prove part (a).

Step 1. Let U be an open normal subgroup of G such that $H \cap U = 1$. We shall show that if $HU \neq G$, then HU/U is an isolated subgroup of G/U.

It suffices to show that if $g \in G$ and $H^g \cap HU \neq 1$, then $g \in HU$. Indeed, if $H^g \cap HU \neq 1$, there exist $h_1, h_2 \in H - \{1\}$ and $u \in U$, such that $h_1^g = h_2 u$. Replacing h_1 by a one of its powers, we may assume that $h_1^p = 1$, where p is a prime divisor of $|H|$. Since $H \cap U = 1$, it follows that $h_2^p = 1$. By Lemma 4.6.4(b), we deduce that $\langle h_1 \rangle = \langle h_2 \rangle$. Put $H_0 = \langle h_1 \rangle$ and $\Gamma = H_0 U$. Clearly, $\Gamma^g = \Gamma$. Since H_0 is a p-Sylow subgroup of Γ, there exists $u_0 \in U$ with $H_0^g = H_0^{u_0}$. Then $1 \neq H_0 \leq H^{g u_0^{-1}} \cap H$; therefore, since H is isolated, $g u_0^{-1} \in H$, i.e., $g \in HU$, as desired.

Step 2. Next we show the existence of a normal complement of H in G.

Choose an open normal subgroup K of G maximal with respect to the property that $H \cap K = 1$. We claim that $HK = G$. Otherwise, HK/K is isolated in G/K by Step 1. Hence (see Theorem 4.6.1), HK/K has a normal complement R/K in G/K, where $K < R \triangleleft_o G$. Then $H \cap R = 1$, contradicting the maximality of K. This proves the claim. So, K is the desired complement.

Step 3. We show that this complement is unique.

Let K and K' be two normal complements of H in G. Consider the collection $\mathcal{V}$ of all open normal subgroups V of G such that $V \leq K \cap K'$. For each $V \in \mathcal{V}$, $G/V = (K/V) \rtimes (HV/V) = (K'/V) \rtimes (HV/V)$. By Step 1, HV/V is an isolated subgroup of the finite group G/V. Hence $K/V = K'/V$ (see Theorem 4.6.1). Thus, $K = K'$ (see Corollary 1.1.8).

This proves part (a). Part (b) is clear from the argument in Step 3. □

Let π be a set of prime numbers. Recall that a supernatural number n is a π-number if the primes involved in n are in π. If G is a profinite group, let $\pi(G)$ denote the set of primes involved in the order $\#G$ of G.

Corollary 4.6.6 *Let G be a profinite group, H a closed isolated Hall subgroup of G and let K the unique normal complement of H in G. Then,*

(a) $K = [G - (\bigcup_{g \in G} H^g)] \cup \{1\}$;
(b) *If $1 \neq k \in K$, then the centralizer $\mathrm{C}_G(k)$ of k in G is contained in K.*

Proof. Clearly H^g is isolated for every $g \in G$ and its normal complement is K. By Lemma 4.6.3, H^g acts fixed-point-free on K. So, part (b) follows from part (a). To prove (a), note that $G = K \rtimes H$ and $\#K$ and $\#H$ are coprime. Hence,

$$K \subseteq \left[G - \left(\bigcup_{g \in G} H^g \right) \right] \cup \{1\}.$$

Conversely, let $1 \neq x \in G - (\bigcup_{g \in G} H^g)$ and assume that $x \notin K$. Since $\bigcup_{g \in G} H^g$ is a compact subset of G, there exists an open normal subgroup V of G such that $V < K$ and

$$xV \cap \left(\bigcup_{g \in G} H^g \right) V = \emptyset.$$

By Lemma 4.6.5, $G/V = K/V \rtimes H$ is a Frobenius group with isolated subgroup H (we are identifying H with its canonical image in G/V). Put $\tilde{x} = xV$. Then $\tilde{x} \notin K/V$; therefore $\tilde{x} \in H^{\tilde{g}}$, for some $g \in G$. This would imply that

$$x \in H^g V \subseteq \left(\bigcup_{g \in G} H^g \right) V,$$

a contradiction. Thus $x \in K$. □

Lemma 4.6.7 *Let G be a profinite group, let K be a closed Hall normal subgroup of G and let H be a complement of K in G. Then H acts (by conjugation) fixed-point-free on K if and only if H acts (by the induced action) fixed-point-free on every finite quotient $K/(K \cap U)$, where $U \triangleleft_o G$.*

Proof. By Lemmas 4.6.3 and 4.6.4, H is isolated and finite. Let $\mathcal{U}$ be the collection of all open normal subgroups of G. Suppose H acts fixed-point-free on $K/(K \cap U)$ for each $U \in \mathcal{U}$, and let $k \in K$ be such that $k^h = k$ for some $1 \neq h \in H$. For $U \in \mathcal{U}$, put $K_U = K \cap U$. Then, obviously $(K_U k)^h = K_U k$ for all $U \in \mathcal{U}$. Hence, $K_U k = K_U$; i.e., $k \in K_U$ for all $U \in \mathcal{U}$. Thus, $k = 1$. The converse follows from Proposition 2.3.16. □

Lemma 4.6.8 *Let $G = K \rtimes H$ be a finite Frobenius group with isolated subgroup H. Assume that a proper quotient $\tilde{G} = H/N$ of H is a Frobenius group with isolated subgroup H_1. Then H_1 is cyclic.*

Proof. Say $\tilde{G} = H/N = K_1 \rtimes H_1$, where K_1 is the Frobenius kernel of $\tilde{G}$. We claim that K_1 contains a subgroup C, characteristic in $\tilde{G}$, such that C is either cyclic of prime order or H_1 has odd order and $C \cong C_2 \times C_2$. Assume the claim holds. Since H_1 acts on K_1 fixed-point-free (see Theorem 4.6.1), this means that H_1 is isomorphic to a subgroup of $\mathrm{Aut}(C)$. If C is cyclic of order p, this will insure that H_1 is cyclic (we remark that in this case, $p \neq 2$, for otherwise, $\mathrm{Aut}(C) = 1$, and this would imply that H_1 is trivial). Finally, observe that $\mathrm{Aut}(C_2 \times C_2) \cong S_3$; hence, if in addition the order of H_1 is odd, then $H_1 \cong C_3$, proving the lemma.

To prove the claim, we distinguish two cases. Assume first that there exists a prime $p \neq 2$ such that $p \mid |K_1|$. Since the p-Sylow subgroups of H are cyclic (see Theorem 4.6.1), so are the p-Sylow subgroups of K_1. Since K_1 is nilpotent, it follows that K_1 contains a cyclic nontrivial characteristic p-Sylow subgroup; and hence a characteristic subgroup of order p.

Assume now that $|K_1|$ is a power of 2 (consequently, $|H_1|$ is odd). Then K_1 cannot be cyclic, as remarked above. Since the 2-Sylow subgroups of H are either cyclic or generalized quaternion, it follows that K_1 is a proper quotient of a generalized quaternion group, say,

$$Q = \langle x, y \mid x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, x^y = x^{-1} \rangle.$$

Let M be a proper nontrivial normal subgroup of Q such that $K_1 = Q/M$. If $\langle x \rangle M = Q$, then K_1 would be cyclic, a contradiction. If $\langle x \rangle M \neq Q$, then $M \leq \langle x \rangle$, since $\langle x \rangle$ is a maximal subgroup in Q. In this case, we have three possibilities:

(1) $M = \langle x \rangle$. Then K_1, would be cyclic, a contradiction.
(2) $M = \langle x^2 \rangle$. Then $K_1 = C_2 \times C_2$.
(3) $M < \langle x^2 \rangle$. Then, since $M \neq 1$, we have that $y^2 = x^{2^{n-2}} \in M$. Therefore, K_1 is dihedral, and so its center is isomorphic to $C_2 \times C_2$. Thus K_1 contains a characteristic subgroup of the form $C_2 \times C_2$. □

The following theorem gives equivalent characterizations of profinite Frobenius groups.

Theorem 4.6.9 *Let G be a profinite group. Then the following conditions are equivalent.*

(a) *G is a profinite Frobenius group*;
(b) *G has a finite isolated Hall subgroup*;
(c) *G is an inverse limit of a surjective inverse system $\{G_i, \varphi_{ij}, I\}$ of finite Frobenius groups*;
(d) *$G = K \rtimes H$, where $\#H$ and $\#K$ are relatively prime and the action of H on K is fixed-point-free*;
(e) *G has a closed Hall normal subgroup K such that $\mathrm{C}_G(k) \leq K$ for every $1 \neq k \in K$.*

Proof. By Lemma 4.6.4, (a) and (b) are equivalent.

(b) ⇒ (c) follows from Lemma 4.6.5.

(c) ⇒ (d) We may assume that G is an infinite group. For each $i \in I$, write $G_i = K_i H_i$, where K_i is the Frobenius kernel of the finite group G_i and where H_i is a Frobenius complement. Consider the subset

$$J = \{j \in I \mid \mathrm{Ker}(\varphi_{ij}) \leq K_i \text{ for all } i \succeq j\}$$

of I. Then J is cofinal in I. To see this, let $r \in I - J$; since G is infinite, there exists some $j \in I$ with $j \succ r$ and $\mathrm{Ker}(\varphi_{jr}) > K_j$. If $j \notin J$, there would exist some $i \in I$ with $i \succ j$ and $\mathrm{Ker}(\varphi_{ij}) > K_i$. By Lemma 4.6.8, H_j is cyclic; hence $G_r = \varphi_{jr}(H_j)$ cannot be a Frobenius group, a contradiction. So $j \in J$.

Therefore, from now on we may assume that $\mathrm{Ker}(\varphi_{ij}) \leq K_i$ for all pairs $i, j \in I$ with $i \succeq j$. For each $i \in I$, let $\mathcal{S}_i$ be the set of all Frobenius complements in G_i. It follows that φ_{ij} induces a map $\mathcal{S}_i \longrightarrow \mathcal{S}_j$. Hence the $\mathcal{S}_i$ form an inverse system of nonempty finite sets. So, there exists some

$$(H_i') \in \varprojlim \mathcal{S}_i.$$

Put $K = \varprojlim K_i$ and $H = \varprojlim H_i'$. Therefore, $G = KH$, $K \triangleleft G$ and $\#K$ and $\#H$ are coprime (see Lemma 2.3.4). By Lemma 4.6.7, H acts fixed-point-free on K.

(d) ⇒ (b) By Lemma 4.6.3, H is isolated. So this implication follows from Lemma 4.6.5.

(a) ⇒ (e) follows from Corollary 4.6.6.

(e) ⇒ (a) By Theorem 2.3.15, $G = K \rtimes H$ for some closed subgroup H of G. The assumption on K implies that H acts fixed-point-free on K. Thus, by Lemma 4.6.3, H is isolated. □

It is known (cf. Huppert [1967], Remark V.8.8) that if K is the Frobenius kernel in a finite Frobenius group G, then K is nilpotent and its class is bounded by a function which depends only on the size of the primes involved in a Frobenius complement H in G. If follows from Lemma 4.6.5 that a Frobenius kernel in a profinite Frobenius group is also nilpotent, and its nilpotency class is bounded by the same function. We record this in the following

Corollary 4.6.10 *Let $G = K \rtimes H$ be a profinite Frobenius group with Frobenius kernel K. Then K is nilpotent. Moreover,*

(a) *If $2 \mid |H|$, then K is abelian;*
(b) *If $3 \mid |H|$, then K is nilpotent of class at most 2;*
(c) *If p is an odd prime and $p \mid |H|$, then K is nilpotent of class at most*

$$\frac{(p-1)^{2^{p-1}-1}-1}{p-2}.$$

4.7 Torsion in the Profinite Completion of a Group

Let G be a group. Define $tor(G)$ to be the set of elements in G of finite order. We refer to $tor(G)$ as the *torsion subset of* G or the *torsion of* G, and to its elements as the torsion elements of G. In this section we study the relationship between the torsion of a residually finite group G and the torsion $tor(\widehat{G})$ of its profinite completion $\widehat{G}$. More precisely, we regard G as a subgroup of $\widehat{G}$ and we are interested in determining for which groups G the closure $\overline{tor(G)}$ in $\widehat{G}$ of $tor(G)$ contains (or coincides with) $tor(\widehat{G})$. In particular, we want to know for which torsion-free groups the profinite completion is torsion-free as well. Note that for a residually finite group G, one always has

$$tor(G) \subseteq tor(\widehat{G}).$$

Furthermore, if the set of orders of the torsion elements of G is bounded, then

$$\overline{tor(G)} \subseteq tor(\widehat{G}).$$

We begin with abelian groups.

Proposition 4.7.1 *Let G be a residually finite abelian group. Then*

$$\overline{tor(G)} \supseteq tor(\widehat{G}).$$

Proof. We use additive notation for G. Let h be an element in $\widehat{G}$ of order $n \in \mathbf{N}$. We must show that for every subgroup U of finite index in G there is a torsion element g_U of G such that $g_U + \overline{U} = h + \overline{U}$. Choose $g \in G$ with $g + \overline{U} = h + \overline{U}$. Then $ng \in \overline{U} \cap G = U$. We claim that $ng \in nU$. Suppose not. Note that G/nU is residually finite, because it has finite exponent and therefore it is a direct sum of finite cyclic groups (cf. Theorem 10.1.5 and Exercise 10.1.2 in Kargapolov and Merzljakov [1979]). Therefore, there exists a subgroup of finite index V in U such that $nU \leq V$ and $ng \notin V$. Choose $g_1 \in G$ such that $g_1 + \overline{V} = h + \overline{V}$. Then $ng_1 \in \overline{V} \cap G = V$ and $g - g_1 \in \overline{U} \cap G = U$. It follows that $n(g - g_1) \in nU \leq V$, so that $ng \in V$, a contradiction. This proves the claim. Thus $ng = nu$ for some $u \in U$. Put $g_U = g - u$. Then $g_U + \overline{U} = g + \overline{U} = h + \overline{U}$ and $ng_U = 0$, as desired. □

Next we give an example of a residually finite abelian group G where $\overline{tor(G)}$ contains $tor(\widehat{G})$ properly.

Example 4.7.2 Let $G = \bigoplus_p \mathbf{Z}/p\mathbf{Z}$, where p ranges through the set of all prime numbers. Clearly G is residually finite and $\widehat{G} = \prod_p \mathbf{Z}/p\mathbf{Z}$. Observe that $\overline{tor(G)} = \widehat{G} \supset tor(\widehat{G})$.

Our next objective is to prove the equality $\overline{tor(G)} = tor(\widehat{G})$ for residually finite minimax solvable groups. Recall that a group is called *minimax* if it has a subnormal series

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

of finite length whose factor groups satisfy either the maximal or the minimal condition on subgroups. One can find information on minimax groups in Robinson [1972]. Note that the class of minimax groups is closed under taking subgroups, homomorphic images and extensions. We start with a description of abelian minimax groups which can be found in Robinson [1972], Lemma 10.31.

Proposition 4.7.3 *An abelian minimax group is an extension of a finitely generated abelian group by a direct product of finitely many quasicyclic groups. Moreover, its torsion subgroup is a direct factor.*

From this one easily deduces the following,

Corollary 4.7.4 (a) *Every abelian minimax group of finite exponent is finite.*
(b) *The torsion subgroup of a residually finite abelian minimax group is finite.*

The following description of solvable minimax groups is given in Robinson [1972], Theorem 10.33.

Theorem 4.7.5 *Let G be a solvable minimax group, let R be the subgroup generated by all quasicyclic subgroups of G and let F/R be the Fitting subgroup of G/R; then*

(a) *R is the direct product of finitely many quasicyclic subgroups of G and R is the intersection of all subgroups of finite index in G,*
(b) *F/R is nilpotent,*
(c) *G/F is polycyclic and abelian-by-finite.*

Lemma 4.7.6 *Let G be a solvable-by-finite minimax group and let H be a normal subgroup of G which is closed in the profinite topology on G. Then the profinite topology of G induces the full profinite topology on H.*

Proof. We have to show that if $N \triangleleft_f H$, then there exists some $U \leq_f G$ such that $N \geq H \cap U$. One checks easily that it is enough to prove the corresponding property for any subgroup of finite index in G. Hence, we may assume that G is a solvable minimax group.

We claim that it suffices to show that any subgroup N of finite index in H is closed in the profinite topology of G. Indeed, in that case, $N = \bigcap_{V \in \mathcal{V}} V$, where $\mathcal{V}$ is the collection of subgroups of finite index in G containing N (see Proposition 2.1.4); since $[H : N] < \infty$, it would follow that $H \cap V = N$, for some $V \in \mathcal{V}$, proving the claim. Now, let $n = [H : N]$ and let H^n be the subgroup of H generated by the n-th powers of the elements of H. Then $H^n \leq N$. Since G is solvable minimax, so is H/H^n. Therefore, H/H^n has a subnormal series whose factor groups are abelian minimax of exponent at most n, and hence finite (see Corollary 4.7.4). Thus, H^n has finite index in H. So, $\{H^n \mid n = 1, 2, \ldots\}$ is a fundamental system of neighborhoods in the profinite topology of H. Therefore, it suffices to show that H^n is closed in the profinite topology of G ($n \in \mathbf{N}$). Now, since H is closed, G/H is residually finite, and so it has no nontrivial quasicyclic subgroups by Theorem 4.7.5. Since H/H^n is finite, G/H^n does not have nontrivial quasicyclic subgroups. Thus, by Theorem 4.7.5(a), G/H^n is residually finite and hence H^n is closed in G as required. □

Lemma 4.7.7 *If A is a residually finite torsion free abelian minimax group, then the group $\widehat{A}/A$ is torsion free and divisible.*

Proof. Since A is torsion free, so is $\widehat{A}$ by Proposition 4.7.1. Let n be a positive integer. Then A/nA is finite by Corollary 4.7.4. Hence $n\widehat{A} \cap A = nA$ (this follows from Proposition 3.2.2). One deduces that $\widehat{A}/A$ is torsion free. Now, if $a_1, \ldots, a_t$ is a transversal of nA in A, we have that $\widehat{A} = \bigcup_{i=1}^t \overline{nA + a_i} = \bigcup_{i=1}^t n\widehat{A} + a_i$; hence $\widehat{A} = n\widehat{A} + A$. Thus, $\widehat{A}/A$ is divisible. □

Theorem 4.7.8 *Let G be a residually finite solvable minimax group. Then*

(a) *Every finite subgroup of $\widehat{G}$ is conjugate to a subgroup of G, and*
(b) $tor(\widehat{G}) = \overline{tor(G)}$.

Proof. First we show that there exists a series of finite length of closed (in the profinite topology of G) normal subgroups of G, whose factors are either finite abelian or torsion-free abelian groups. The existence of such a series can be established as follows: since G is solvable, it admits a normal series

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

whose factor groups G_{i+1}/G_i are abelian; we shall refer to such a series as a solvable series of length n. We proceed by induction on the length n of such a series. If $n = 1$, G is abelian; then $tor(G)$ is finite (see Corollary 4.7.4) and hence closed in the profinite topology of G; moreover $G/tor(G)$ is torsion-free. Assume that $n > 1$. Put $A = G_1$. Then the closure $\mathrm{Cl}(A)$ of A in G is a residually finite abelian minimax group; hence $tor(\mathrm{Cl}(A))$ is finite, $tor(\mathrm{Cl}(A)) \triangleleft G$ and $\mathrm{Cl}(A)/tor(\mathrm{Cl}(A))$ is torsion-free. On the other hand, $G/\mathrm{Cl}(A)$ has a solvable series of length $n-1$; hence, by induction, there is a series of closed normal subgroups from $\mathrm{Cl}(A)$ to G whose factor groups are either finite abelian or torsion-free abelian. Putting these two series together, we get a normal series for G of the desired type.

It follows that the set of orders of the elements in $tor(G)$ is bounded. So, $\overline{tor(G)} \subseteq tor(\widehat{G})$. On the other hand, since $tor(G)$ is invariant under conjugation in G, the set $\overline{tor(G)}$ is invariant under conjugation in $\widehat{G}$. Thus, part (b) is an immediate consequence of (a).

We shall prove part (a) by induction on the length of a series

$$1 = A_0 \leq A_1 \leq \cdots \leq A_m = G \tag{4}$$

of closed normal subgroups of G each of whose factors is either a finite abelian group or a torsion-free abelian group. The result holds if $m = 1$ by Proposition 4.7.1 and the fact that $tor(G)$ is finite. Assume that the result is true for residually finite solvable minimax groups admitting a series of this type of length $m = k$, and let G be a residually finite solvable minimax group with a series (4) of this type of length $m = k + 1$. Let $A = A_1$. If A is torsion, then it is finite; since the result holds for G/A by the induction hypothesis, it also holds for G in this case.

Therefore we may assume that A is torsion-free. Put $Q = G/A$. Since A is closed in the topology of G, one deduces that Q is residually finite. Let H be a finite subgroup of $\widehat{G}$. We must show that H is conjugate to a subgroup of G. By Lemma 4.7.6, the profinite topology of G induces on A its own profinite topology; hence by Lemma 3.2.6 and Proposition 3.2.5, the sequence

$$1 \longrightarrow \widehat{A} \longrightarrow \widehat{G} \longrightarrow \widehat{Q} \longrightarrow 1$$

is exact. So $\widehat{Q}$ can be identified with $\widehat{G}/\widehat{A}$. Note that the image of H in $\widehat{Q}$ is conjugate to a subgroup of $Q = G\widehat{A}/\widehat{A}$ by the induction hypothesis. Hence $H^g\widehat{A} \le G\widehat{A}$, for some $g \in \widehat{G}$. Replacing H by H^g we may assume that $H \le G\widehat{A}$. Since both G and $\widehat{A}$ normalize A it follows that H normalizes A. Thus we can view A and $\widehat{A}$ as left H-modules via the action of H by conjugation:

$$h \cdot a = hah^{-1} \quad (h \in H, a \in \widehat{A}).$$

For each $h \in H$, there exist some $g_h \in G$, $a_h \in \widehat{A}$ such that $h = a_h g_h$. Although a_h is not uniquely determined by h, it is uniquely determined modulo A (for, if $a_h g_h = a'_h g'_h$, then $a_h^{-1} a'_h = (g'_h)^{-1} g_h \in A$, because $\widehat{A} \cap G = A$, since A is closed in the profinite topology of G).

We claim that the function $\delta : H \longrightarrow \widehat{A}/A$ defined by $\delta(h) = a_h A$ is a derivation (see Section 6.8). Indeed, let $h_1, h_2 \in H$ and say $h_1 = a_1 g_1$ and $h_2 = a_2 g_2$, with $a_i \in \widehat{A}$, $g_i \in G$ $(i = 1, 2)$; then,

$$h_1 h_2 = a_1(g_1 a_2 g_1^{-1}) g_1 g_2 = a_1(h_1 a_2 h_1^{-1}) g_1 g_2 = a_1(h_1 \cdot a_2) g_1 g_2;$$

hence

$$\delta(h_1 h_2) = (h_1 \cdot (a_2 A))(a_1 A) = (h_1 \cdot \delta(h_2))\delta(h_1).$$

By Lemma 4.7.7, $\widehat{A}/A$ is torsion-free and divisible. Hence, $H^1(H, \widehat{A}/A) = 0$ (see Corollary 6.7.5). Therefore δ is an inner derivation (see Lemma 6.8.1), i.e., there exists some $b \in \widehat{A}$ such that

$$\delta(h) = (h \cdot (bA))(bA)^{-1}, \quad \text{for all } h \in H.$$

Therefore,

$$a_h A = hbh^{-1}b^{-1}A, \quad \text{for all } h \in H.$$

Since $h^{-1}a_h = g_h^{-1} \in G$, we deduce that $bhb^{-1} \in G$ for all $h \in H$, i.e., $bHb^{-1} \le G$. Thus H is conjugate to a subgroup of G. □

A group G is *polycyclic* if it has a subnormal series of finite length whose factor groups are cyclic. Such a group is residually finite (cf. Robinson [1996], Corollary 5.4.17) and it is obviously solvable minimax. Clearly, finitely generated nilpotent groups are polycyclic. The following corollary is an immediate consequence of the theorem above.

Corollary 4.7.9 *Let G be a polycyclic group. Then $\overline{tor(G)} = tor(\widehat{G})$.*

Next we state a result which extends Proposition 4.7.1 to finitely generated abelian by nilpotent groups. The proof can be found in Kropholler and Wilson [1993].

Theorem 4.7.10 *Let G be a finitely generated abelian by nilpotent group (i.e., a group having an abelian normal subgroup with nilpotent quotient). Then $\overline{tor(G)} = tor(\widehat{G})$.*

We finish the section by showing that the profinite completion of a torsion-free finitely generated residually finite group need not be torsion-free in general. Before we establish this, we introduce some terminology and recall some facts about the special linear group $\mathrm{SL}_n(\mathbf{Z})$.

(i) $\mathrm{SL}_n(\mathbf{Z}) = \langle I + e_{ij} \mid 1 \leq i, j \leq n, i \neq j \rangle$, where I is the identity matrix of size n, and e_{ij} denotes the $n \times n$ matrix with 1 as entry ij and zeroes elsewhere. (This is proved using the Euclidean algorithm for $\mathbf{Z}$ and the fact that pre- or post-multiplication of a matrix by e_{ij} corresponds to elementary row or column operations on the matrix.)

(ii) The natural homomorphism $\mathrm{SL}_n(\mathbf{Z}) \longrightarrow \mathrm{SL}_n(\mathbf{Z}/m\mathbf{Z})$ is onto for $m = 1, 2, \ldots$. (This follows easily from (i).)

(iii) The groups of the form

$$\Gamma_n(m) = \mathrm{Ker}(\mathrm{SL}_n(\mathbf{Z}) \longrightarrow \mathrm{SL}_n(\mathbf{Z}/m\mathbf{Z}))$$

are called *congruence subgroups* of $\mathrm{SL}_n(\mathbf{Z})$. For a fixed n, denote by $\mathcal{N}$ the collection of all congruence subgroups $\Gamma_n(m)$ $(m = 1, 2, \ldots)$. Then $\mathcal{N}$ is a fundamental system of neighborhoods for a Hausdorff topology on $\mathrm{SL}_n(\mathbf{Z})$, the *congruence subgroup topology*. It is easy to prove with the help of (ii) that if we denote by $\mathcal{K}_{\mathcal{N}}(\mathrm{SL}_n(\mathbf{Z}))$ the completion of $\mathrm{SL}_n(\mathbf{Z})$ with respect to the congruence subgroup topology, then

$$\mathcal{K}_{\mathcal{N}}(\mathrm{SL}_n(\mathbf{Z})) = \varprojlim_{m \in \mathbf{N}} \mathrm{SL}_n(\mathbf{Z}/m\mathbf{Z}) \cong \mathrm{SL}_n(\widehat{\mathbf{Z}}) \cong \prod_p \mathrm{SL}_n(\mathbf{Z}_p).$$

(iv) One may compare the congruence topology on $\mathrm{SL}_n(\mathbf{Z})$ with its profinite topology. The *congruence subgroup problem* over $\mathbf{Z}$ is the problem of deciding whether these two topologies coincide. One may state the problem in the following equivalent form. Consider the natural continuous epimorphism

$$\varphi : \widehat{\mathrm{SL}_n(\mathbf{Z})} \longrightarrow \mathrm{SL}_n(\widehat{\mathbf{Z}}).$$

Then the congruence subgroup problem is the problem of deciding whether the kernel of φ is trivial. In Bass, Lazard and Serre [1964] and Mennicke [1965] it is shown that if $n \geq 3$, then $\mathrm{Ker}(\varphi) = 1$, i.e., the profinite and the congruence subgroup topologies on $\mathrm{SL}_n(\mathbf{Z})$ coincide. For $n = 2$, it was known at that time that the two topologies are different: we give a precise description of $\mathrm{Ker}(\varphi)$ for the case $n = 2$ in Theorem 8.8.1. See Rapinchuk [1999] for a survey of the congruence subgroup problem in a more general setting.

Lemma 4.7.11 *Let $n \geq 2$ and $m \geq 3$. Then $\Gamma_n(m)$ is torsion-free.*

Proof. If $p \mid m$, then $\Gamma_n(m) \leq \Gamma_n(p)$. So, we may assume that $m = p$ is a prime number. Let $\alpha \in \Gamma_n(p)$; then $\alpha = I + p^r \beta$, where I is the identity matrix, β is an $n \times n$ matrix over $\mathbf{Z}$ with at least one entry not divisible by p, and where r is a natural number ≥ 1. Let t be a positive integer. Say $t = p^s u$, with s and u natural numbers and $p \nmid u$. Then

$$\alpha^t = (I + p^r\beta)^t = I + \binom{t}{1} p^r\beta + \cdots = I + p^{r+s}u\beta + p^{r+s+1}\gamma,$$

for a certain $n \times n$ matrix γ. Thus $\alpha^t \neq I$. □

Proposition 4.7.12 *Given any finite group K, there exists a finitely generated torsion-free linear group G whose profinite completion contains a direct product $\prod_{\aleph_0} K$ of countably many copies of K.*

Proof. Fix an integer $n \geq 3$. As pointed out above, the congruence and the profinite topologies of $\mathrm{SL}_n(\mathbf{Z})$ coincide in that case, so that $\widehat{\mathrm{SL}_n(\mathbf{Z})}$ can be identified with $\prod_p \mathrm{SL}_n(\mathbf{Z}_p)$. From the properties stated above, it is clear that the congruence subgroup $\Gamma_n(m)$ is residually finite, it has finite index in $\mathrm{SL}_n(\mathbf{Z})$ and it is finitely generated. Moreover, $\Gamma_n(m)$ is torsion-free if $m \geq 3$ by Lemma 4.7.11.

Now, the profinite completion $\widehat{\Gamma_n(m)}$ of $\Gamma_n(m)$ can be regarded as an open subgroup of $\widehat{\mathrm{SL}_n(\mathbf{Z})} = \mathrm{SL}_n(\widehat{\mathbf{Z}})$ (see Proposition 3.2.2). Therefore, by the definition of the product topology, it contains a direct factor of the form $\prod_{p \notin \Sigma} \mathrm{SL}_n(\mathbf{Z}_p)$, where Σ is a finite set of primes. Since $\mathrm{SL}_n(\mathbf{Z})$ contains the permutation group S_n and since K is finite, one can find n such that $\mathrm{SL}_n(\mathbf{Z})$ contains a copy of K. Therefore, for each p, $\mathrm{SL}_n(\mathbf{Z}_p)$ contains a copy of K. Thus $\widehat{\Gamma_n(m)}$ contains $\prod_{\aleph_0} K$. □

An example of a finitely generated residually finite torsion-free group whose completion contains every countably based profinite group will be given in Corollary 9.4.6.

4.8 Notes, Comments and Further Reading

Theorem 4.2.2 was first proved for finitely generated pro-p groups by J-P. Serre (in an unpublished letter to A. Pletch, dated March 26, 1975) using Lie algebra methods. Anderson [1976] extended Serre's result to finitely generated abelian-by-pronilpotent profinite groups. Oltikar and Ribes [1978] proved the result for finitely generated prosupersolvable groups. Theorem 4.2.7 in the form presented here is due to Hartley [1979]. Part (b) of Proposition 4.2.9 is based on an argument of Rhemtulla [1969]. Proposition 4.2.3 and Corollary 4.2.4 are also due to Anderson. Example 4.2.12 is due to Peterson [1973]; he also proves that an uncountably generated (i.e., a nonmetrizable) profinite group is never strongly complete. Proposition 4.2.13 was proved by Pletch [1981]. In Saxl and Wilson [1997] and Martínez and Zel'manov [1996] it is shown that finitely generated profinite groups that are direct products of finite simple groups are strongly complete.

A prosolvable version of Theorem 4.2.2 was proved by Segal [2000]; he gives an explicit formula for the function $f(d)$ described in Lemma 4.2.1 in the case of the commutator word, namely

Theorem 4.8.1 *In a finite d-generated solvable group H, every element of the derived subgroup $[H,H]$ is equal to the product of $f(d) = 72d^2 + 45d$ commutators.*

In Nikolov and Segal [2007a, 2007b] they prove

Theorem 4.8.2 *Let G be a finitely generated profinite group and H is a closed normal subgroup of G. Then $[H,G]$ is closed in G. In particular, any term $\gamma_n(G)$ of the lower central series of G is closed.*

However the terms of the derived series (other than the commutator subgroup) of a finitely generated profinite group are not closed in general. Examples of this are provided in Roman'kov [1982]. In the case of pro-p groups Jaikin-Zapirain [2008] proves the following

Theorem 4.8.3 *Let F be a free nonabelian pro-p group of finite rank, and let w be a group word, $1 \neq w \in \Phi$, where Φ is a free abstract group. Then $w(F)$ is closed in F if and only if $w \notin [\Phi,\Phi]^p[[\Phi,\Phi],[\Phi,\Phi]]$.*

A related question was suggested by A. Shalev.

Open Question 4.8.4 *Let G be a finitely generated profinite group and let n be a natural number. Let $\langle G^n\rangle = \langle x^n \mid x \in G\rangle$ be the subgroup of G generated by the nth powers of its elements. Is $\langle G^n\rangle$ closed?*

Note that a positive answer to this question combined with the solution of Burnside's problem given by E. Zel'manov for profinite groups (see below) would give another proof of Theorem 4.2.2. Indeed, let H be a normal subgroup of index n in a finitely generated profinite group G. If $\langle G^n\rangle$ is closed, then $G/\langle G^n\rangle$ is a finitely generated torsion group. By a result of Zel'manov (Zel'manov [1992], Theorem 1), $G/\langle G^n\rangle$ is finite. Hence $\langle G^n\rangle$ would be open in G. On the other hand, $\langle G^n\rangle \leq H$; thus H would be open as well.

Martínez [1996] gives a positive answer to this question when G is a pro-$\mathcal{N}^\ell$ group; see also Martínez [1994]. More generally, Nikolov and Segal [2007a, 2007b] answer this question positively for groups G for which there exists at least one finite group not isomorphic to an open section B/A of G, (i.e., with $A \triangleleft B \leq G$ and A open in G).

An infinite profinite group is called *just-infinite* if it is infinite and if every nontrivial closed normal subgroup is open (see, e.g., Wilson [2000]). Jaikin-Zapirain [2002] proves that if G is a nonsolvable just-infinite pro-p group, then every nontrivial normal subgroup of G is open.

The monograph of Segal [2009] contains an excellent exposition on results about group words; many of them relate to whether certain verbal subgroups of profinite groups are closed.

4.8.5 Profinite Torsion Groups

The following theorem is proved by Hewitt and Ross [1970] (Theorem 28.20).

Theorem 4.8.5a *Every compact Hausdorff torsion group is profinite.*

In the same location they mention the following question, which they seem to consider to be folklore at the time.

Open Question 4.8.5b *Is a torsion profinite group necessarily of finite exponent?*

The Burnside Problem for finitely generated compact Hausdorff torsion groups was raised by Platonov [1966]; see also in Kourovka [1984]: every finitely generated profinite torsion group is finite. This conjecture has been proved to be correct in the case of finitely generated pro-p groups by Zel'manov. Using methods in the theory of Lie algebras developed in Zel'manov [1990] and Zel'manov [1991], he proves

Theorem 4.8.5c (Zel'manov [1992], Theorem 1) *Every finitely generated pro-p torsion group is finite.*

In fact Platonov's conjecture has a positive answer for all finitely generated profinite groups. This can be seen by combining the above theorem of Zel'manov with a reduction due to Wilson and Herfort to the case of pro-p groups. This reduction is a consequence of the following

Theorem 4.8.5d (Wilson [1983], Theorem 1) *Let G be a profinite torsion group. Then G has a finite series*

$$1 = G_n \leq G_{n-1} \leq \cdots \leq G_0 = G$$

of closed characteristic subgroups such that each group G_i/G_{i+1} is either a pro-p group, for some prime p, or a direct product of isomorphic finite simple groups.

The theorem of Wilson in turn is based on a previous result of Herfort.

Theorem 4.8.5e (Herfort [1980], Theorem 1) *Let G be a profinite torsion group. Then the order of G is divisible by only finitely many distinct primes.*

A somewhat related result is the following

Theorem 4.8.5f (Herfort [1982]) *Let G be a profinite group whose order is divisible by infinitely many different primes. Then G contains a procyclic subgroup with the same property.*

Another consequence of the theorem of Zel'manov mentioned above is that every infinite compact Hausdorff group contains an infinite abelian subgroup (see Zel'manov [1992], Theorem 2). In this connection see also McMullen [1974].

The first description of the automorphism group of a finitely generated profinite group (Corollary 4.4.4) that we are aware of appears in Smith [1969]. A different proof of Theorem 4.4.7 describing $\mathrm{Aut}(\mathbf{Z}_p)$ is given in Serre [1973], Proposition II.8.

The abstract version of Lemma 4.5.2 is due to Hall [1958]. The abstract version of Lemma 4.5.3 was proved by Andreadakis [1965]. Proposition 4.5.1 and Theorem 4.5.6 are due to Lubotzky [1982].

Anderson [1974] proves a result more general than Lemma 4.5.5, namely, he shows that if G a finitely generated profinite group which is virtually pro-p, then $\mathrm{Aut}(G)$ is also virtually pro-p.

4.8.6 Normal Automorphisms

A continuous automorphism $\varphi : G \longrightarrow G$ of a profinite group G is called *normal* if $\varphi(N) = N$ for every open normal subgroup N of G. Neukirch [1969] proved that every automorphism of the absolute Galois group $G_{\bar{\mathbf{Q}}/\mathbf{Q}}$ of $\mathbf{Q}$ is normal. He conjectured that in fact every automorphism of $G_{\bar{\mathbf{Q}}/\mathbf{Q}}$ is inner. This conjecture was proved by Uchida [1976] and by Ikeda [1977]. In Jarden and Ritter [1980] a corresponding result is proved for $G_{\bar{K}/K}$, where K is any finite extension of the field $\mathbf{Q}_p$ of p-adic numbers. In Jarden [1980] he considers an analogous question for free profinite groups, and he proves the following

Theorem 4.8.6a *Let H and J be open subgroups of the nonabelian free profinite group F. Suppose that $\sigma : H \to J$ is an isomorphism such that $\sigma(U) = U$ for every open normal subgroup U of F contained in $H \cap J$. Then σ is induced by an inner automorphism of F.*

The results in Section 4.6 dealing with infinite profinite Frobenius groups are due to Gildenhuys, Herfort and Ribes [1979].

The question about existence of torsion in the profinite completion of residually finite torsion-free groups was raised in Crawley-Boevey, Kropholler and Linnell [1988], where the absence of torsion in the profinite completion of a torsion-free solvable-by-finite minimax group and a torsion-free metabelian-by-finite group was proved. The first example of a residually finite torsion-free group whose profinite completion has torsion was discovered by Evans [1990]. Proposition 4.7.1 is due to Chatzidakis. The results 4.7.2 and 4.7.6–4.7.8 are due to Kropholler and Wilson [1993]. In this paper they construct examples of finitely generated torsion-free center-by-metabelian groups whose profinite completion contains torsion.

For results about prop-p center-by-metabelian groups see Kochloukova and Pinto [2008]. For the probability of generating a prosolvable group, see Lucchini, Menegazzo and Morigi [2006].

Proposition 4.7.12 was proved by Lubotzky [1993]; he also gives an example of a finitely generated residually finite torsion-free group whose completion contains every countably based profinite group.

Chatzidakis [1999] proves the existence of a two-generated torsion-free residually finite p-group whose pro-p completion contains every countably based pro-p group.

One may pose a dual problem to the one considered above: let G be an infinite finitely generated residually finite torsion group. Is $\widehat{G}$ torsion? The answer to this is always negative. This follows from the result of Zel'manov quoted in Theorem 4.8.5c and the reduction results of Wilson and Herfort (4.8.5d and 4.8.5e above). For a special case of this see McMullen [1985].

5 Discrete and Profinite Modules

5.1 Profinite Rings and Modules

A *profinite ring* Λ is an inverse limit of an inverse system $\{\Lambda_i, \varphi_{ij}\}$ of finite rings. We always assume that rings have an identity element, denoted usually by 1, and that homomorphisms of rings send identity elements to identity elements. A profinite ring Λ is plainly a compact, Hausdorff and totally disconnected topological ring; the converse is also true, as we indicate in Proposition 5.1.2 below. It is clear that a profinite ring admits a fundamental system of neighborhoods of 0 consisting of open (two-sided) ideals (this follows from a result analogous to Lemma 2.1.1).

Let Λ be a profinite ring. An abelian Hausdorff topological group M is said to be a *left Λ-module* if there is a continuous map $\Lambda \times M \to M$, denoted by $(\lambda, m) \mapsto \lambda m$, satisfying the following conditions

(i) $(\lambda_1\lambda_2)m = \lambda_1(\lambda_2 m)$
(ii) $(\lambda_1 + \lambda_2)m = \lambda_1 m + \lambda_2 m$
(iii) $\lambda(m_1 + m_2) = \lambda m_1 + \lambda m_2$
(iv) $1m = m$

for $m, m_1, m_2 \in M$ and $\lambda, \lambda_1, \lambda_2 \in \Lambda$, where 1 is the identity element of Λ.

Similarly, a *right Λ-module* is defined as a topological abelian group M together with a continuous map $M \times \Lambda \to M$ denoted by $(m, \lambda) \mapsto m\lambda$, satisfying conditions analogous to (i), (ii), (iii) and (iv) above.

If Λ is a profinite ring, Λ^{op} will denote the opposite ring, that is a ring with the same elements and the same addition as Λ, and where the multiplication $\circ$ is defined by $m_1 \circ m_2 = m_2 m_1$. Clearly Λ^{op} is also a profinite ring. Any right Λ-module can be thought of as a left Λ^{op}-module in a natural way; hence, any general statement about left Λ-modules is also valid for right Λ-modules. We often refer to left Λ-modules simply as *Λ-modules*.

If M and N are two Λ-modules, we use the notation $\mathrm{Hom}_\Lambda(M, N)$ for the abelian group of all continuous Λ-homomorphisms $M \longrightarrow N$ from M to N; $\mathrm{Hom}(M, N)$ denotes the abelian group of all continuous homomorphisms from M to N as abelian profinite groups. We sometimes write $\mathrm{End}_\Lambda(M)$ and $\mathrm{End}(M)$ for $\mathrm{Hom}_\Lambda(M, M)$ and $\mathrm{Hom}(M, M)$, respectively. For convenience, sometimes we refer to a continuous Λ-homomorphism of Λ-modules as a *morphism of Λ-modules*.

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4_5,

Sometimes we want to think of $\mathrm{Hom}_\Lambda(M,N)$ as a topological group; in that case it is understood that its topology is the compact-open topology (see Section 2.9).

We leave to the reader the development of the natural notions of submodule of a module, quotient module M/N of a module M modulo a submodule N, kernel and image of a morphism of Λ-modules, etc.

Let X be a subset of a Λ-module M. The closed Λ-submodule generated by X is the intersection of all closed Λ-submodules of M containing X; we denote it by $\overline{\langle X\rangle}$. We say that M is *finitely generated* if $M = \overline{\langle X\rangle}$ for some finite subset X of M. As in the case of profinite groups, we say that a subset Y of a profinite Λ-module M *converges to* 1 if every open submodule of M contains all but finitely many elements of Y; a map $\varphi : X \longrightarrow M$ from a set X into a profinite group M *converges to* 1 if the set $\varphi(X)$ converges to 1 in M.

Lemma 5.1.1 *Let Λ be a profinite ring and let M be a Λ-module.*

(a) *If M is discrete, then M is the union of its finite Λ-submodules; in particular, M is torsion as an abelian group.*
(b) *If M is profinite, then it is the inverse limit of its finite quotient Λ-modules. Equivalently, the submodules of M of finite index form a fundamental system of neighborhoods of* 0*.*
(c) *Every profinite Λ-module contains a subset of generators converging to* 1*.*

Proof. Let M be discrete and let $m \in M$. Since there exists a fundamental system of neighborhoods of 0 in Λ consisting of open ideals of Λ, there is an open ideal T of Λ such that $Tm = 0$; therefore, Λm is a submodule with finitely many elements. Thus (a) follows.

To prove (b) we first think of M simply as an abelian profinite group with respect to addition. As such, its open subgroups form a fundamental system of neighborhoods of the element 0 (see Theorem 2.1.3). Next we prove that if U is an open subgroup of the abelian group M, then it contains some open Λ-submodule. By continuity of the action of Λ on M, for each $\lambda \in \Lambda$ there exists some open neighborhood W_λ of λ in Λ and some open subgroup V_λ of U such that $W_\lambda V_\lambda \subseteq U$. Since Λ is compact, there exist finitely many elements $\lambda_1, \dots, \lambda_t \in \Lambda$ such that $W_{\lambda_1}, \dots, W_{\lambda_t}$ is a covering of Λ. Put $V = \bigcap_{i=1}^t V_{\lambda_i}$. Then $V \le_o U$ and $\Lambda V \subseteq U$. Let N be the closure of the subgroup of U consisting of all finite sums of the form $\lambda_1 v_1 + \cdots + \lambda_r v_r$ ($\lambda_i \in \Lambda, v_i \in V$). Then N is an open Λ-module contained in U, as needed.

Consider the collection $\{N_i \mid i \in I\}$ of all open Λ-submodules of M. One readily checks that

$$M = \varprojlim M/N_i$$

(see the implication (c) $\Rightarrow$ (d) in Theorem 2.1.3).

Part (c) follows from Proposition 2.4.4. □

Note that in the proof of (b) above we only use the compactness of Λ and the fact that M is a compact, Hausdorff and totally disconnected group. A slight modification of the proof of the above lemma shows that a compact Hausdorff totally disconnected ring is the inverse limit of finite rings, i.e., it is profinite. To be complete we collect several useful characterizations of profinite rings in the following proposition.

Proposition 5.1.2 *Let Λ be a topological ring. Then the following conditions are equivalent.*

(a) *Λ is a profinite ring*;
(b) *Λ is compact and Hausdorff*;
(c) *Λ is compact, Hausdorff and totally disconnected*;
(d) *Λ is compact and the zero element of Λ has a fundamental system of neighborhoods consisting of open ideals of Λ*;
(e) *The zero element of Λ has a fundamental system of neighborhoods $\{T_i \mid i \in I\}$ consisting of open ideals of Λ, and $\Lambda = \varprojlim \Lambda/T_i$*;
(f) *There is an inverse system $\{\Lambda_i, \varphi_{ij}\}$ of finite rings, where each morphism φ_{ij} is an epimorphism, and $\Lambda = \varprojlim \Lambda_i$.*

Proof. Most of the proof is done by mimicking the proof of Theorem 2.1.3; we leave the details to the reader. The only new fact is the implication (b) $\Rightarrow$ (c), and we proceed to establish this. We wish to prove that the connected component C of 0 in Λ is $\{0\}$. To prove this, consider the Pontryagin dual $\Lambda^* = \mathrm{Hom}(\Lambda, \mathbf{Q}/\mathbf{Z})$ of Λ as a compact abelian group (see Section 2.9). Then Λ^* is a discrete abelian group, and we make it into a Λ-module by the rule $(\lambda f)(\mu) = f(\mu\lambda)$ $(\lambda, \mu \in \Lambda, f \in \Lambda^*)$. Now, for any $f \in \Lambda^*$, $Cf = \{cf \mid c \in C\}$ is a continuous image of C, and so it is a connected subset of Λ^*. Since Λ^* is discrete, $Cf = 0$. Hence $0 = (cf)(1) = f(c)$ for each $c \in C$, i.e., $f(C) = 0$. Since this is valid for every $f \in \Lambda^*$, one deduces as a consequence of the Pontryagin-van Kampen duality theorem for compact abelian groups that $C = 0$ (cf. Hewitt and Ross [1963], Theorem 24.10 or Hofmann and Morris [2006], Theorem 7.64, for example). □

Exercise 5.1.3 (The structure of commutative profinite rings)

(1) *Finite rings*: Let R be a commutative finite ring and let $\{P_1, \dots, P_n\}$ be the collection of its maximal ideals.
  (1i) Prove that for every natural number $m = 1, 2, \dots$, $P_i^m + P_j^m = R$ whenever $i \neq j$. Deduce that $\bigcap_{i=1}^n P_i^m = P_1^m \cdots P_n^m$.
  (1ii) Prove that there exists a natural number m such that the homomorphism
$$R \longrightarrow R/P_1^m \times \cdots \times R/P_n^m$$
given by $r \mapsto (r + P_1^m, \dots, r + P_n^m)$ is an isomorphism. (Hint: recall that the Jacobson radical $J(R) = \bigcap_{i=1}^n P_i$ of Λ is nilpotent;

choose m to be the smallest positive integer such that $0 = J(R)^m (= P_1^m \cdots P_n^m)$.)

(1iii) Prove that R is a direct product of local rings (recall that a ring is called *local* if it has a unique maximal ideal).

(2) *Commutative profinite rings*: A commutative profinite ring R is the direct product of profinite local rings. (Hint: show that an epimorphism of finite commutative rings $\varphi : R_1 \longrightarrow R_2$ sends a system $\{P_1, \ldots, P_n, R_1; m\}$, consisting of the maximal ideals of R_1, the ring R_1, and a natural number m such that $P_1^m \cdots P_n^m = 0$, to another system of the same type.)

The class of all Λ-modules together with their morphisms form an abelian category (cf. Mac Lane [1963] for a formal definition of the concept of abelian category). In particular if $M_1, \ldots, M_t$ is a collection of finitely many Λ-modules, there exists a *direct sum* $\bigoplus_{i=1}^t M_i$ of these modules which is a Λ-module, namely, the set of all t-tuples $(m_1, \ldots, m_t)$ $(m_i \in M_i, i = 1, \ldots, t)$ with the product topology and the usual definition of coordinatewise addition and multiplication by elements of Λ.

Let $\varphi : \Lambda \longrightarrow \Lambda'$ be a continuous homomorphism of profinite rings. If A' is a Λ'-module, it becomes a Λ-module via φ by the action $\lambda a' = \varphi(\lambda) a'$ $(a' \in A', \lambda \in \Lambda)$. Let A be a Λ-module and let $f : A \to A'$ (respectively, $f : A' \to A$) be a continuous homomorphism of groups. We say that the pair φ, f of maps is *compatible* if f is a map of Λ-modules, i.e., if $f(\lambda a) = \varphi(\lambda) f(a')$ (respectively, $f(\varphi(\lambda) a') = \lambda f(a')$) for all $a \in A$, $\lambda \in \Lambda$, $a' \in A'$.

Lemma 5.1.4

(a) *Let $\{\Lambda_i, \varphi_{ij}\}$ be an inverse system of profinite rings over a directed poset $(I, \preceq)$; for each $i \in I$ let A_i be a profinite Λ_i-module and B_i a discrete Λ_i-module. Assume that $\{A_i, f_{ij}\}$ is an inverse system of profinite abelian groups, and $\{B_i, g_{ij}\}$ a direct system of discrete abelian groups with the additional conditions that for each pair $i, j \in I$ with $i \succeq j$, both f_{ij} and g_{ji} are compatible with φ_{ij}, and moreover f_{ij} and φ_{ij} are epimorphisms. Put*
$$\Lambda = \varprojlim \Lambda_i, \qquad A = \varprojlim A_i, \quad \text{and} \quad B = \varinjlim B_i.$$
Then A and B are Λ-modules, and the natural homomorphism
$$\Psi : \varinjlim \mathrm{Hom}_{\Lambda_i}(A_i, B_i) \longrightarrow \mathrm{Hom}_{\Lambda}(A, B)$$
is an isomorphism (the topologies of $\mathrm{Hom}_{\Lambda}(A, B)$ and $\mathrm{Hom}_{\Lambda_i}(A_i, B_i)$ are assumed to be the compact-open topologies; in this case these are discrete topologies).

(b) *Let Λ be a profinite ring, $\{A_i, \alpha_{ij}\}$ an inverse system of profinite Λ-modules over an indexing set I, and $A = \varprojlim A_i$. Let B be a discrete Λ-module and write it as a direct limit $\varinjlim_{j \in J} B_j$ of finitely generated Λ-submodules of B. Then there is a natural isomorphism*

$$\Delta : \mathrm{Hom}_\Lambda(B, A) \longrightarrow \varprojlim_{I,J} \mathrm{Hom}_\Lambda(B_j, A_i).$$

(*this is in fact a topological isomorphism; in this case the compact-open topologies of* $\mathrm{Hom}_\Lambda(B, A)$ *and* $\mathrm{Hom}_\Lambda(B_j, A_i)$ *are compact, Hausdorff and totally-disconnected*).

(c) *Let* Λ *and* B *be as in part* (b). *Then* $\mathrm{Hom}_\Lambda(B, -)$ *commutes with inverse limits, i.e., if* $\{A_i, \alpha_{ij}\}$ *is as in* (b), *then there is a natural* (*topological*) *isomorphism*

$$\mathrm{Hom}_\Lambda(B, A) \longrightarrow \varprojlim_{I} \mathrm{Hom}_\Lambda(B, A_i).$$

Proof. (a) Let $f_i : A \to A_i$, $g_i : B_i \to B$ and $\varphi_i : \Lambda \to \Lambda_i$ denote the canonical mappings ($i \in I$). First we indicate the action of Λ on A and B. If $\lambda = (\lambda_i) \in \Lambda$ and $a = (a_i) \in A$ ($\lambda_i \in \Lambda_i, a_i \in A_i, i \in I$), then define $\lambda a = (\lambda_i a_i)$. If $b \in B$, choose $i \in I$ and $b_i \in B_i$ so that $g_i(b_i) = b$; then put $\lambda b = g_i(\lambda_i b_i)$; this is well-defined by the compatibility of the maps φ_{ij} and g_{ji}. Next we make the homomorphisms

$$\Phi_{ij} : \mathrm{Hom}_{\Lambda_i}(A_i, B_i) \to \mathrm{Hom}_{\Lambda_j}(A_j, B_j) \quad (i \preceq j)$$

and

$$\Psi_i : \mathrm{Hom}_{\Lambda_i}(A_i, B_i) \to \mathrm{Hom}_\Lambda(A, B)$$

explicit: if $h_i \in \mathrm{Hom}_{\Lambda_i}(A_i, B_i)$, define $\Phi_{ij}(h_i) = g_{ij} h_i f_{ji}$ and $\Psi_i(h_i) = g_i h_i f_i$. Let $\Phi_i : \mathrm{Hom}_{\Lambda_i}(A_i, B_i) \to \varinjlim \mathrm{Hom}_{\Lambda_i}(A_i, B_i)$ be the canonical maps. The homomorphisms Ψ_i commute with the Φ_{ij}, and so they induce the map Ψ in the statement. We show that this map is both injective and surjective, and thus an isomorphism.

Ψ *is injective*: Assume $h \in \varinjlim \mathrm{Hom}_{\Lambda_i}(A_i, B_i)$ with $\Psi(h) = 0$, and let $k \in I$ and $h_k \in \mathrm{Hom}_{\Lambda_i}(A_k, B_k)$ be such that $\Phi_k(h_k) = h$ (see Proposition 1.2.4). For $i \succeq k$, let $h_i = \Phi_{ki}(h_k)$; then $0 = \Psi(h) = \Psi_i(h_i) = g_i h_i f_i$. If $i \succeq k$, define

$$X_i = \{a_i \in A_i \mid h_i(a_i) \neq 0\}.$$

We shall show that for some $i \succeq k$, $X_i = \emptyset$, i.e., $h_i = 0$; this will imply that $h = 0$, as needed. Since h_i is continuous, A_i compact and B_i discrete, one has that h_i takes only a finite number of values; hence X_i is closed and, therefore compact. On the other hand $i \succeq j \succeq k$ implies that $f_{ij}(X_i) \subseteq X_j$. Indeed, if $a_i \in X_i$, then $0 \neq h_i(a_i) = (g_{ji} h_j f_{ij})(a_i)$. So $h_j(f_{ij}(a_i)) \neq 0$; hence $f_{ij}(a_i) \in X_j$. Therefore,

$$\{X_i, f_{ij} \mid i, j \succeq k\}$$

is an inverse system of compact spaces. Now, if

$$a \in \varprojlim_{i \geq k} X_i \subseteq A,$$

then $\Psi(h)(a) = \Psi_i(h_i)(a) = (g_i h_i f_i)(a) = (g_i h_i)(a_i)$; since $h_i(a_i) \neq 0$ if $i \succeq k$, it follows from Proposition 1.2.4, that $\Psi(h)(a) \neq 0$. Since by assumption $\Psi(h) = 0$, we deduce that

$$\varprojlim_{i \geq k} X_i = \emptyset.$$

Thus, by Proposition 1.1.4, there is some i such that $X_i = \emptyset$, as asserted.

Ψ is surjective: Let $h \in \operatorname{Hom}_\Lambda(A, B)$. We shall show that for some $i \in I$ there exists $h_i \in \operatorname{Hom}_{\Lambda_i}(A_i, B_i)$ such that $h = \Psi(h_i) = g_i h_i f_i$. Notice that since A is compact and B discrete, $h(A)$ is finite. Hence, there exists $j_0 \in I$ such that for every $j \succeq j_0$ there is some Λ_j-submodule D_j of B_j for which the restriction of g_j maps D_j isomorphically onto $h(A)$ (one sees this using Proposition 1.2.4(ii) and the fact that each B_k is torsion). Since $h(A)$ is finite, $\operatorname{Ker}(h)$ is open in A. Hence (replacing j_0 by a larger index if necessary) there exists an open Λ_{j_0}-submodule U_{j_0} with $U = f_{j_0}^{-1}(U_{j_0}) \leq \operatorname{Ker}(h)$. For $j \succeq j_0$, define $U_j = f_{jj_0}^{-1}(U_{j_0})$; then

$$A/U = \varprojlim_{j \geq j_0} A_j/U_j.$$

Since A/U is finite and each $A/U \longrightarrow A_j/U_j$ is an epimorphism, there exists $i \succeq j_0$ such that the canonical map $A/U \longrightarrow A_i/U_i$ is an isomorphism. Let $\bar{h} : A/U \longrightarrow B$ be the map induced by h. Then there is a unique (Λ_i-homomorphism) $\bar{h}_i : A_i/U_i \longrightarrow D_i$ such that the diagram

$$\begin{array}{ccccc} A/U & \xrightarrow{\bar{h}} & h(A) & \hookrightarrow & B \\ \downarrow{\cong} & & \uparrow & & \\ A_i/U_i & \xrightarrow{\bar{h}_i} & D_i & & \end{array}$$

commutes. Let h_i be the composition $A_i \longrightarrow A_i/U_i \xrightarrow{\bar{h}_i} D_i \hookrightarrow B_i$. This h_i is the desired map.

(b) First let us make Δ explicit. Define

$$\Delta_{ij} : \operatorname{Hom}_\Lambda(B, A) \longrightarrow \operatorname{Hom}_\Lambda(B_j, A_i)$$

as follows: if $h \in \operatorname{Hom}_\Lambda(B, A)$, then $h_{ij} = \Delta_{ij}(h)$ is the result of restricting h to B_j and composing this with the canonical map $A \longrightarrow A_i$. By the definition of the topologies involved, it is plain that each Δ_{ij} is continuous. Hence these maps induce a continuous homomorphism Δ. Suppose that $\Delta(h) = 0$. Then $h_{ij} = 0$ for every $i \in I, j \in J$. Therefore $h = 0$. This shows that Δ is an injection. Consider now an element (h_{ij}) of $\varprojlim \operatorname{Hom}_\Lambda(B_j, A_i)$. For a fixed $i \in I$, define $h_i : B \longrightarrow A_i$ as follows: if $b \in B$, then choose B_j such that $b \in B_j$ and put $h_i(b) = h_{ij}(b)$. Set $h = \varprojlim h_i$. Then $\Delta(h) = (h_{ij})$. The proof of (c) is similar. □

We shall be particularly interested in two types of Λ-modules M: those that are compact, Hausdorff and totally disconnected (i.e., profinite), and those that are discrete. We refer to the first type as *profinite modules*, and to the second as *discrete modules*. Profinite Λ-modules together with their morphisms form an category that we shall denote by $\mathbf{PMod}(\Lambda)$. The category of discrete Λ-modules and their morphisms will be denoted by $\mathbf{DMod}(\Lambda)$. It is easy to verify that both $\mathbf{PMod}(\Lambda)$ and $\mathbf{DMod}(\Lambda)$ are abelian subcategories of the category of all Λ-modules.

Duality Between Discrete and Profinite Modules

Next we generalize the construction made in the proof of Proposition 5.1.2. Given a Λ-module M (discrete or profinite), consider the abelian group $M^* = \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$ of all continuous homomorphism from M to $\mathbf{Q}/\mathbf{Z}$ (as abelian groups) with the compact open topology (see Section 2.9). By Theorem 2.9.6, M^* is profinite if M discrete torsion, and it is discrete torsion if M is profinite. Define a right action of Λ on M^* by $(\varphi\lambda)(m) = \varphi(\lambda m)$. This action is continuous and so M^* becomes a right Λ-module, i.e., a Λ^{op}-module. Therefore, it easily follows from Theorem 2.9.6 and the definition of action that the contravariant functor $\mathrm{Hom}(-, \mathbf{Q}/\mathbf{Z})$ establishes a "duality" between the categories $\mathbf{PMod}(\Lambda)$ and $\mathbf{DMod}(\Lambda^{op})$. In other words, for every Λ-module M in $\mathbf{PMod}(\Lambda)$ or $\mathbf{DMod}(\Lambda)$, there is a continuous Λ-isomorphism

$$M \longrightarrow M^{**},$$

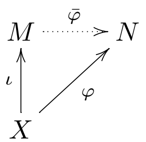
of Λ-modules; furthermore, this isomorphism is natural in the sense that if $\varphi : M \longrightarrow N$ is a morphism in either $\mathbf{PMod}(\Lambda)$ or $\mathbf{DMod}(\Lambda)$, then the diagram

$$\begin{array}{ccc} M & \longrightarrow & M^{**} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi^{**}} \\ N & \longrightarrow & N^{**} \end{array}$$

commutes, where φ^{**} is the map obtained from φ by applying the functor $\mathrm{Hom}(-, \mathbf{Q}/\mathbf{Z})$ twice. It is important to understand the implications of this duality since we shall make use of them often. For a precise statement of duality see for example Mac Lane [1963]. In our context duality can be described as follows: every (elementary) statement, definition, theorem, etc., that one makes in either the category $\mathbf{PMod}(\Lambda)$ or $\mathbf{DMod}(\Lambda^{op})$ involving modules and morphisms (that we represent by arrows), can be translated into a dual statement, definition, theorem, etc. in the other category by applying the functor $\mathrm{Hom}(-, \mathbf{Q}/\mathbf{Z})$, i.e., replacing each module M by $\mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$ and reversing the arrows; if a statement, theorem, etc., holds in one of these categories, then the dual statement, theorem, etc. holds true in the other category.

5.2 Free Profinite Modules

Let X be a profinite space, Λ a profinite ring, M a profinite Λ-module and $\iota : X \longrightarrow M$ a continuous mapping. We say that (M, ι) is a *free profinite* Λ-module on the space X or, simply, M is a free profinite Λ-module on X, if the following universal property is satisfied:



whenever $\varphi : X \longrightarrow N$ is a continuous mapping into a profinite Λ-module N, there exists a unique continuous homomorphism $\bar{\varphi} : M \longrightarrow N$ such that the above diagram commutes, i.e., $\bar{\varphi}\iota = \varphi$.

A free profinite Λ-module on a pointed topological space $(X, *)$ is defined similarly. It consists of a profinite Λ-module M together with a map of pointed spaces $\iota : (X, *) \longrightarrow M$ (i.e., $\iota(*) = 0$) satisfying an analogous universal property: whenever $\varphi : X \longrightarrow N$ is a continuous mapping of pointed spaces into a profinite Λ-module N, there exists a unique continuous homomorphism $\bar{\varphi} : M \longrightarrow N$ such that $\bar{\varphi}\iota = \varphi$.

Another way of expressing this is the following. Let N be a topological Λ-module and let $\mathrm{C}(X, N)$ denote the set of all continuous mappings from X to N. Then M is a free profinite Λ-module on X if and only if the natural map

$$\mathrm{Hom}(M, N) \longrightarrow \mathrm{C}(X, N)$$

induced by ι is a bijection for each profinite Λ-module N. Similarly for a free Λ-module on a pointed space $(X, *)$.

Observe that one needs to test the above universal property (or, equivalently, the existence of the above bijection) only for finite Λ-modules N, for then it holds automatically for any profinite Λ-module N, since N is an inverse limit of finite Λ-modules (see Lemma 5.1.1).

Lemma 5.2.1 *Let Λ be a profinite ring and let (M, ι) be a free profinite Λ-module on the profinite space X (respectively, a free profinite Λ-module on the profinite pointed space $(X, *)$), then*

(a) *$\iota(X)$ generates M as a Λ-module*;
(b) *The mapping ι is injective.*

Proof. The proof of part (b) is essentially the same as the proof of Lemma 3.3.1, and we leave it to the reader. We prove part (a) for a free profinite Λ-module (M, ι) on a profinite space X; the pointed case is similar. Let N be the closed Λ-submodule of M generated by $\iota(X)$. By the universal property of (M, ι), there exists a continuous homomorphism $\varphi : M \longrightarrow M$

such that $\varphi\iota = \iota$; and so $\varphi(M) = N$. On the other hand, it is clear that the identity map id_M on M also satisfies the condition $(\mathrm{Id}_M)\iota = \iota$. Hence $\varphi = \mathrm{id}_M$, and thus $M = N$. □

From these definitions it is easily deduced that if a free profinite Λ-module exists, then it is unique. We shall denote the free profinite Λ-module on X by $[\![\Lambda X]\!]$, and the free profinite Λ-module on the pointed space $(X,*)$ by $[\![\Lambda(X,*)]\!]$.

If X is a set and Λ a ring, we denote the abstract free Λ-module on X by $[\Lambda X]$. Hence, $[\Lambda X]$ is simply the direct sum $\bigoplus_X \Lambda$ of copies of Λ (considered as a Λ-module) indexed by X. Note that if X is finite and Λ is a profinite ring, then $[\![\Lambda X]\!] = [\Lambda X]$. Similarly, if $(X,*)$ is finite, then $[\![\Lambda(X,*)]\!] = [\Lambda(X,*)] = \bigoplus_{X-\{*\}} \Lambda$.*

Proposition 5.2.2 *Let Λ be a profinite ring.*

(a) *For every profinite space X, there exists a unique free profinite Λ-module $[\![\Lambda X]\!]$ on X, namely $[\![\Lambda X]\!] = \varprojlim [\Lambda X_j]$, where $X = \varprojlim X_j$ is any decomposition of X as an inverse limit of finite spaces.*
(b) *For every profinite pointed space $(X,*)$, there exists a unique free profinite Λ-module $[\![\Lambda(X,*)]\!]$ on the pointed space $(X,*)$, namely $[\![\Lambda(X,*)]\!] = \varprojlim [\Lambda(X_j,*)]$, where $(X,*) = \varprojlim (X_j,*)$ is any decomposition of $(X,*)$ as an inverse limit of finite pointed spaces.*

Proof. (a) As pointed out above, the uniqueness follows immediately from the definition, and we leave it to the reader. We begin with the construction of $[\![\Lambda X]\!]$. If X is finite, it is clear that $[\![\Lambda X]\!] = [\Lambda X] = \bigoplus_X \Lambda$. Assume that X is infinite. Write $X = \varprojlim X_j$, where $\{X_i, \varphi_{ij}, I\}$ is a surjective inverse system of finite spaces. Denote by $\rho_j : X \longrightarrow X_j$ the canonical projections. Then the free profinite Λ-modules $[\Lambda X_j]$ constitute an inverse system. Define $[\![\Lambda X]\!] = \varprojlim [\Lambda X_j]$. Let $\iota\colon X \longrightarrow [\![\Lambda X]\!]$ be the inverse limit of the natural homomorphisms $X_j \longrightarrow [\Lambda X_j]$. Next we show that $([\![\Lambda X]\!], \iota)$ is a free profinite Λ-module on X. Indeed, let N be a finite Λ-module, and let $\varphi\colon X \longrightarrow N$ be continuous. Since $\varphi(X)$ is finite, φ factors through some $\rho_j : X \longrightarrow X_j$, i.e. there exists a $\varphi'\colon X_j \longrightarrow N$ with $\varphi'\rho_j = \varphi$ (see Lemma 1.1.16). Since $[\Lambda X_j]$ is a free profinite Λ-module on X_j, φ' can be extended to a Λ-module homomorphism $\overline{\varphi'} : [\Lambda X_j] \longrightarrow N$. Put $\bar\varphi = \overline{\varphi'}\psi_j$, where $\psi_j : [\![\Lambda X]\!] \longrightarrow [\Lambda X_j]$ is the projection. It is easy to see that $\bar\varphi\iota = \varphi$, as required.

* Some authors use the notation ΛX or even $\Lambda[X]$ for what we denote $[\Lambda X]$. The first one is fine if one is only dealing with abstract free modules, while $\Lambda[X]$ might be confused with the notation normally used for rings of polynomials. Our notation allows us to distinguish between such free modules and profinite free modules $[\![\Lambda X]\!]$. We shall make later similar distinctions when dealing with group algebras and complete group algebras.

Finally it follows from uniqueness that the above construction of $[\![\Lambda X]\!]$ is independent of how X is written as an inverse limit of finite spaces.

(b) The proof for this part is similar. $\square$

We shall refer to the profinite space X (respectively, $(X,*)$) as a topological *basis* of $[\![\Lambda X]\!]$ (respectively, of $[\![\Lambda(X,*)]\!]$).

Exercise 5.2.3 Let $\{\Lambda_i, \varphi_{ij}\}$ $\{X_i, \psi_{ij}\}$ and $\{(Y_i,*), \rho_{ij}\}$ be inverse systems of profinite rings, profinite spaces and pointed profinite spaces, respectively, over a poset I. Let $\Lambda = \varprojlim \Lambda_i$, $X = \varprojlim X_i$ and $(Y,*) = \varprojlim (Y_i,*)$. Then

$$[\![\Lambda X]\!] = \varprojlim [\![\Lambda_i X_i]\!] \quad \text{and} \quad [\![\Lambda(Y,*)]\!] = \varprojlim [\![\Lambda_i(Y_i,*)]\!].$$

Exercise 5.2.4 Let Λ be a profinite ring. Let Y and Z be closed subspaces of the profinite pointed space $(X,*)$ such that $* \in Y$ and $* \notin Z$.

(a) Prove that the natural Λ-homomorphisms $[\![\Lambda Z]\!] \longrightarrow \overline{\langle Z\rangle}$ and $[\![\Lambda(Y,*)]\!] \longrightarrow \overline{\langle Y\rangle}$ are isomorphisms; so $\overline{\langle Z\rangle}$ can be identified with $[\![\Lambda Z]\!]$ and $\overline{\langle Y\rangle}$ with $[\![\Lambda(Y,*)]\!]$.
(b) Show that there is an isomorphism $[\![\Lambda(X,*)]\!]/[\![\Lambda(Y,*)]\!] \cong [\![\Lambda(X/Y,*)]\!]$.
(c) Prove that $(Y,*) = \bigcap_{i\in I}(Y_i,*)$ implies $[\![\Lambda(Y,*)]\!] = \bigcap_{i\in I}[\![\Lambda(Y_i,*)]\!]$, where the $(Y_i,*)$ are closed subsets of $(X,*)$.
(d) Prove that assertions analogous to (a), (b) and (c) also hold in the non-pointed case.

(Hint: use the decomposition $[\![\Lambda(X,*)]\!] = \varprojlim[\Lambda(X_j,*)]$ and note that the assertions are obvious if X is finite.)

Let S be a set and let us think of it as a discrete space. Let $\bar{S} = S \cup \{*\}$ be its one-point compactification. We shall refer to $[\![\Lambda(\bar{S},*)]\!]$ as the free profinite Λ-module on the set S converging to 0. We denote it by $[\![\Lambda S]\!]$ (with a certain abuse of notation; to avoid any ambiguity, whenever we use this notation for this purpose, we shall specify that it is a module on the set S converging to 0). Then one easily proves the following result.

Lemma 5.2.5 *Let S be a set.*

(a) *The Λ-module $[\Lambda S]$ is a dense submodule of the free profinite Λ-module $[\![\Lambda S]\!]$ on the set S converging to* 0.
(b) *The free profinite Λ-module $[\![\Lambda S]\!]$ on the set S converging to* 0 *is characterized by the following universal property: whenever $\varphi : S \longrightarrow M$ is a mapping converging to* 0 *of S into a profinite Λ-module M, then there exists a unique continuous Λ-homomorphism*

$$\bar{\varphi} : [\![\Lambda S]\!] \longrightarrow M$$

such that $\bar{\varphi}(s) = \varphi(s)$ for every $s \in S$.
(c) *Every Λ-module is a quotient of a free profinite Λ-module on a set converging to* 0.

5.3 G-modules and Complete Group Algebras

Let G be a profinite group. A *left G-module* or simply a *G-module* is a topological abelian group M on which G operates continuously. Specifically, a G-module is a topological abelian group M together with a continuous map $G \times M \to M$, denoted by $(g, a) \mapsto ga$, satisfying the following conditions

(i) $(gh)a = g(ha)$,
(ii) $g(a + b) = ga + gb$,
(iii) $1a = a$,

for $a, b \in M$ and $g, h \in G$, where 1 is the identity of G.

If the topology of M is discrete, then M is called a *discrete G-module*; and if the topology of M is profinite, we say that M is a *profinite G-module. Right G-modules* are defined analogously.

We leave it to the reader to develop the concepts of G-submodule and G-submodule generated by a collection of elements in a G-module.

The following lemma is proved easily.

Lemma 5.3.1 *Let G be a profinite group and let M be a discrete abelian group. Let $G \times M \longrightarrow M$ be an action of G on M satisfying conditions* (i), (ii), (iii) *as above. Then, the following are equivalent*:

(a) $G \times M \longrightarrow M$ *is continuous*;
(b) *For each a in M, the stabilizer*,

$$G_a = \{g \in G \mid ga = a\}$$

of a is an open subgroup of G;
(c)

$$M = \bigcup_U M^U,$$

where U runs through the set of all open subgroups of G, and where

$$M^U = \{a \in M \mid ua = a,\ u \in U\},$$

is the subgroup of fixed points of M under the action of U.

Example 5.3.2 (Discrete G-modules)

(1) Let G be any profinite group and M any discrete abelian group. Define an action of G on M by $ga = a$, for all $a \in M$ and $g \in G$. Then M is a discrete G-module. This action is called the *trivial action* on M, and we refer to M with this action as a *trivial G-module*.
(2) Let N/K be a Galois extension of fields and $G = G_{N/K}$ its Galois group. For $\sigma \in G$ and $x \in N$, define $\sigma x = \sigma(x)$. Under this action the following are examples of discrete G-modules:

(2a) $N^\times$ (the multiplicative group of N);
(2b) N^+ (the additive group of N);
(2c) The roots of unity in N (under multiplication).

As proved in Lemma 5.1.1, discrete modules over a profinite ring must be torsion as abelian groups; in contrast observe that a discrete G-module need not be torsion. For example, with the exception of (2c), the examples above are not torsion abelian groups in general.

Let M and N be G-modules. A *G-morphism* $\varphi : A \longrightarrow B$ is a continuous G-homomorphism, i.e., an abelian group homomorphism for which

$$\varphi(ga) = g\varphi(a), \quad \text{for all } g \in G, a \in M.$$

The class of G-modules and G-morphisms constitutes an abelian category which we denote by $\mathbf{Mod}(G)$. The profinite G-modules form an abelian subcategory of $\mathbf{Mod}(G)$, denoted $\mathbf{PMod}(G)$, while the discrete G-modules form an abelian subcategory denoted $\mathbf{DMod}(G)$. In turn, the discrete torsion G-modules form a subcategory of $\mathbf{DMod}(G)$.

Lemma 5.3.3 *Let G be a profinite group and let M be a G-module.*

(a) *If M is a discrete G-module, then it is finitely generated as a G-module if and only if it is finitely generated as an abelian group.*
(b) *If M is discrete torsion, then it is the union of its finite G-submodules.*
(c) *If M is profinite, then it is an inverse limit of finite G-modules.*

Proof. (a) Suppose $a_1, \ldots, a_t$ are generators of M as a G-module. Let G_i be the stabilizer of a_i $(i = 1, \ldots, t)$. Then G_i is an open subgroup of G (see Lemma 5.3.1). Hence $\bigcup_{i=1}^t Ga_i = \bigcup_{i=1}^t (G/G_i)a_i$ is a finite set of generators of M as an abelian group.

(b) It is plain that if M is discrete, it is the union of its finitely generated submodules. Hence to prove (b) it suffices to show that every finitely generated discrete torsion G-module is finite. This follows from (a) since a finitely generated torsion abelian group is finite.

The proof of (c) is almost identical to the proof of part (b) of Lemma 5.1.1, and we leave it to the reader. □

Exercise 5.3.4 Let G be a profinite group, Λ a profinite ring and M a finite abelian group with the discrete topology. Show that M is a G-module (respectively, an Λ-module) if and only if there exists a continuous group homomorphism (respectively, a continuous ring homomorphism) $G \longrightarrow \mathrm{Aut}(M)$ (respectively, $\Lambda \longrightarrow \mathrm{End}(M)$).

The Complete Group Algebra

Consider a commutative profinite ring R and a profinite group H. We denote the usual abstract group algebra (or group ring) by $[RH]$. Recall that it consists of all formal sums $\sum_{h \in H} r_h h$ ($r_h \in R$, where r_h is zero for all but a finite number of indices $h \in H$), with natural addition and multiplication. As an abstract R-module, $[RH]$ is free on the set H.

Assume that H is a finite group. Then $[RH]$ is (as a set) a direct product $[RH] \cong \prod_H R$ of $|H|$ copies of R. If we impose on $[RH]$ the product topology, then $[RH]$ becomes a topological ring, in fact a profinite ring (since this topology is compact, Hausdorff and totally disconnected). Suppose now that G is a profinite group. Define the *complete group algebra* $[\![RG]\!]$ to be the inverse limit

$$[\![RG]\!] = \varprojlim_{U \in \mathcal{U}} [R(G/U)]$$

of the ordinary group algebras $[R(G/U)]$, where $\mathcal{U}$ is the collection of all open normal subgroups of G. Then $[\![RG]\!]$ is a profinite ring. It is easy to express $[\![RG]\!]$ as an inverse limit of finite rings

$$[\![RG]\!] = \varprojlim [(R/I)(G/U)],$$

where I and U range over the open ideals of R and the open normal subgroups of G, respectively. Consider now the topology on the ring $[RG]$ with a fundamental system of neighborhoods of 0 consisting of the ideals

$$\operatorname{Ker}([RG] \longrightarrow [(R/I)(G/U)])$$

of $[RG]$, where $[RG] \longrightarrow [(R/I)(G/U)]$ are the natural epimorphisms. We refer to that topology as the *natural profinite topology* of $[RG]$. The following lemma is now obvious.

Lemma 5.3.5 *Let G be a profinite group and R a commutative profinite ring.*

(a) *The intersection of all the ideals* $\operatorname{Ker}([RG] \longrightarrow [(R/I)(G/U)])$ *is zero.*
(b) $[\![RG]\!]$ *is the completion of* $[RG]$ *endowed with its natural profinite topology.*
(c) $[RG]$ *is densely embedded in* $[\![RG]\!]$.
(d) *As a module,* $[\![RG]\!]$ *is a free profinite R-module on the underlying profinite space of G.*
(e) $[\![RG]\!]$ *behaves functorially on G.*

Proposition 5.3.6 *Let G be a profinite group and R a commutative profinite ring.*

(a) *Every* $[\![RG]\!]$*-module is naturally a G-module.*
(b) *Every profinite abelian group and every discrete torsion abelian group has a unique* $\widehat{\mathbf{Z}}$*-module structure.*
(c) *Profinite G-modules coincide with profinite* $[\![\widehat{\mathbf{Z}}G]\!]$*-modules.*
(d) *If A is both a G-module and an R-module with commuting actions* (*i.e., if $r \in R$, $g \in G$ and $a \in A$, then $r(ga) = g(ra)$*), *then A is in a natural way an* $[\![RG]\!]$*-module.*

(e) *The category* $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$ *coincides with the subcategory of* $\mathbf{DMod}(G)$ *consisting of the discrete torsion* G*-modules.*

Proof. Part (a) is clear since G is naturally embedded in $[\![RG]\!]$ (see Lemma 5.3.5(c)). Part (b) follows from Lemma 4.1.1.

To prove (c), let M be a profinite G-module. By (b), M has also the structure of a $\widehat{\mathbf{Z}}$-module in a unique way; moreover, if $g \in G, \alpha \in \widehat{\mathbf{Z}}$ and $m \in M$, then $g(\alpha m) = (g\alpha)m$. Express M as a inverse limit

$$M = \varprojlim M_i$$

of finite G-modules M_i. To see that M has a unique $[\![\widehat{\mathbf{Z}}G]\!]$-module structure that induces on M its original G-module structure, it suffices to show that this is the case for each M_i, as one easily checks. Consider the continuous homomorphism

$$G \longrightarrow \mathrm{Aut}(M_i)$$

determined by the G-action (see Exercise 5.3.4). Let U be the kernel of this homomorphism. Then there is a corresponding continuous homomorphism of rings $[\widehat{\mathbf{Z}}(G/U)] \longrightarrow \mathrm{End}(M_i)$; and so a continuous homomorphism of rings

$$[\widehat{\mathbf{Z}}G] \longrightarrow [\widehat{\mathbf{Z}}(G/U)] \longrightarrow \mathrm{End}(M_i),$$

where $[\widehat{\mathbf{Z}}G]$ has its profinite topology. This in turn determines a continuous homomorphism of rings

$$[\![\widehat{\mathbf{Z}}G]\!] \longrightarrow \mathrm{End}(M_i),$$

since $[\![\widehat{\mathbf{Z}}G]\!]$ is the completion of $[\widehat{\mathbf{Z}}G]$; i.e., M_i is a $[\![\widehat{\mathbf{Z}}G]\!]$-module. Furthermore, it follows from this definition that the action of $[\![\widehat{\mathbf{Z}}G]\!]$ on M_i extends the action of G on M_i.

Part (d) is proved similarly. Finally, (e) follows from (c), Lemma 5.1.1 and Lemma 5.3.3. $\square$

5.4 Projective and Injective Modules

Let $\mathfrak{C}$ be a category. An object P in $\mathfrak{C}$ is called *projective* if for every diagram

$$\begin{array}{ccc} & & P \\ & & \downarrow{\scriptstyle \varphi} \\ B & \xrightarrow{\alpha} & A \end{array} \qquad (1)$$

of objects and morphisms in $\mathfrak{C}$, where α is an epimorphism, there exists a morphism $\beta : P \longrightarrow B$ making the diagram commutative, i.e., $\alpha\beta = \varphi$. We refer to β as a *lifting* (of φ). If $\mathfrak{C}$ is an abelian category, one has equivalently, that P is projective in $\mathfrak{C}$ if the functor $\mathrm{Hom}(P, -)$ is exact, i.e., whenever

$$0 \longrightarrow C \longrightarrow B \longrightarrow A \longrightarrow 0$$

is an exact sequence in $\mathfrak{C}$, so is the corresponding sequence

$$0 \longrightarrow \mathrm{Hom}(P, C) \longrightarrow \mathrm{Hom}(P, B) \longrightarrow \mathrm{Hom}(P, A) \longrightarrow 0$$

of abelian groups.

When $\mathfrak{C}$ is the category of profinite modules over a profinite ring, it suffices to use finite Λ-modules A in B in the diagram (1) to test the projectivity of a module P, as the next lemma shows.

Lemma 5.4.1 *Let Λ be a profinite ring and P a profinite Λ-module. Then P is projective in the category* $\mathbf{PMod}(\Lambda)$ *of all profinite Λ-modules if and only if whenever there is a diagram of the form* (1) *in* $\mathbf{PMod}(\Lambda)$, *where α is an epimorphism and A and B are finite, there exists a continuous Λ-homomorphism $\beta : P \longrightarrow B$ making the diagram commutative.*

Proof. In one direction the result is obvious. For the other, consider a general diagram of profinite Λ-modules

$$\begin{array}{ccccc} & & & & P \\ & & & \overset{\beta}{\swarrow} & \downarrow{\scriptstyle \varphi} \\ K & \longrightarrow & B & \xrightarrow{\alpha} & A \end{array}$$

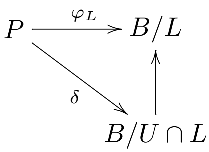
where α is an epimorphism. Denote by K the kernel of α. For every submodule H of B contained in K, let $\alpha_H : B/H \longrightarrow A$ denote the Λ-epimorphism induced by α. Let $\mathcal{E}$ be the collection of all pairs (H, φ_H) where H is a Λ-submodule of B contained in K, and $\varphi_H : P \longrightarrow B/H$ is a continuous Λ-homomorphism such that $\alpha_H \varphi_H = \varphi$. $\mathcal{E}$ is not empty, since $(K, \alpha_K^{-1}\varphi) \in \mathcal{E}$. Define a partial ordering $\preceq$ on $\mathcal{E}$ as follows: $(H, \varphi_H) \preceq (H', \varphi_{H'})$ if $H \geq H'$ and $\varphi_H = \pi\varphi_{H'}$, where $\pi : B/H' \longrightarrow B/H$ is the canonical projection. It is easily seen that $(\mathcal{E}, \preceq)$ is an inductive poset; hence by Zorn's Lemma it has a maximal element, say (L, φ_L). The result will be proved if we can show that $L = 1$. Suppose not; then there exists some open submodule U of B such that $L \cap U < L$. Since both B/U and $B/(U+L)$ are finite and $B/U \longrightarrow B/(U+L)$ is an epimorphism, the map

$$P \xrightarrow{\varphi_L} B/L \longrightarrow B/(U+L)$$

can be lifted to a continuous Λ-homomorphism $\beta : P \longrightarrow B/U$. Remark that

$$\begin{array}{ccc} B/L \cap U & \longrightarrow & B/U \\ \downarrow & & \downarrow \\ B/L & \longrightarrow & B/(U+L) \end{array}$$

is a pullback diagram of Λ-modules. Hence, there exists a map of Λ-modules $\delta : P \longrightarrow B/U \cap L$ such that the diagram



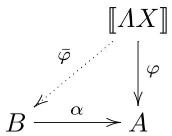
commutes. It follows that $\alpha_{U\cap L}\delta = \varphi$, and so $(U \cap L, \delta) \in \mathcal{E}$, contradicting the maximality of (L, φ_L). Thus $L = 1$ as desired. □

One says that a category $\mathfrak{C}$ has *enough projectives* if for every object M in $\mathfrak{C}$, there exists a projective object P of $\mathfrak{C}$ and an epimorphism $P \longrightarrow M$.

Proposition 5.4.2 *Let Λ be a profinite ring.*

(a) *Every free profinite Λ-module is projective in the category* $\mathbf{PMod}(\Lambda)$ *of all profinite Λ-modules.*
(b) *The category* $\mathbf{PMod}(\Lambda)$ *has enough projectives.*
(c) *The projective objects in* $\mathbf{PMod}(\Lambda)$ *are precisely the direct summands of free profinite Λ-modules.*

Proof. (a) We prove this for free modules over a nonpointed topological space, the pointed case being similar. By Lemma 5.4.1, it suffices to test the projectivity property for finite modules. Let $[\![\Lambda X]\!]$ be a free profinite Λ-module on the profinite space X. Consider a diagram in $\mathbf{PMod}(\Lambda)$



where A and B are finite and α is an epimorphism. Choose a section $\sigma : A \longrightarrow B$ of α (considering α as a set map). Hence by the universal property of free modules, there exists a continuous Λ-homomorphism $\bar{\varphi} : [\![\Lambda X]\!] \longrightarrow B$ such that $\bar{\varphi}(x) = \sigma\varphi(x)$ $(x \in X)$; therefore $\alpha\bar{\varphi} = \varphi$. Thus $\bar{\varphi}$ is a lifting of φ as required.

(b) This follows from part (a) and Lemma 5.2.5.

(c) Let P be a projective profinite Λ-module. By Lemma 5.2.5, there is a free profinite Λ-module $[\![\Lambda X]\!]$ and an epimorphism $\alpha : [\![\Lambda X]\!] \longrightarrow P$. Since P is projective, there exists a continuous Λ-homomorphism $\sigma : P \longrightarrow [\![\Lambda X]\!]$ such that $\alpha\sigma = \mathrm{id}_P$. Therefore, σ is a monomorphism, and by the compactness of P, we have that P is topologically isomorphic to $\sigma(P)$. Then one readily checks that $[\![\Lambda X]\!] = \sigma(P) \oplus \mathrm{Ker}(\alpha)$. □

The dual concept of a projective object in a category $\mathfrak{C}$ is that of an injective object. An object Q in $\mathfrak{C}$ is called *injective* if whenever

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\varphi}\downarrow & & \\ Q & & \end{array} \tag{2}$$

is a diagram of objects and morphisms in $\mathfrak{C}$, where α is a monomorphism, there exists a morphism $\bar{\varphi} : B \longrightarrow Q$ making the diagram commutative, i.e., $\bar{\varphi}\alpha = \varphi$. We refer to $\bar{\varphi}$ as an *extension* of φ. If $\mathfrak{C}$ is an abelian category, one has equivalently, that Q is injective in $\mathfrak{C}$ if the functor $\mathrm{Hom}(-, Q)$ is exact, i.e., whenever

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is an exact sequence in $\mathfrak{C}$, so is the corresponding sequence

$$0 \longrightarrow \mathrm{Hom}(C, Q) \longrightarrow \mathrm{Hom}(B, Q) \longrightarrow \mathrm{Hom}(A, Q) \longrightarrow 0$$

of abelian groups.

Since the categories of profinite projective Λ-modules $\mathbf{PMod}(\Lambda)$ and the category of discrete Λ-modules $\mathbf{DMod}(\Lambda)$ are dual to each other (see Section 4.1), we obtain automatically the following results by duality.

Lemma 5.4.3 *Let Λ be a profinite ring and Q a discrete Λ-module. Then Q is injective in the category* $\mathbf{DMod}(\Lambda)$ *of all discrete Λ-modules if and only if whenever there is a diagram of the form* (2) *in* $\mathbf{DMod}(\Lambda)$, *where α is a monomorphism and A and B are finite, there exists a continuous Λ-homomorphism $\bar{\varphi} : B \longrightarrow Q$ making the diagram commutative.*

One says a category $\mathfrak{C}$ has *enough injectives* if for every object M in $\mathfrak{C}$, there exists an injective object Q of $\mathfrak{C}$ and a monomorphism $M \longrightarrow Q$.

An object M in $\mathbf{DMod}(\Lambda)$ is called *cofree* if it satisfies a universal property dual to that of free objects, i.e., if its dual M^* is free in $\mathbf{PMod}(\Lambda)$. Applying duality, Proposition 5.4.2 yields

Proposition 5.4.4 *Let Λ be a profinite ring.*

(a) *Every cofree discrete Λ-module is injective in the category* $\mathbf{DMod}(\Lambda)$ *of all discrete Λ-modules.*
(b) *The category* $\mathbf{DMod}(\Lambda)$ *has enough injectives.*
(c) *The injective objects in* $\mathbf{DMod}(\Lambda)$ *are precisely the direct factors of cofree discrete Λ-modules.*

Let G be a profinite group. Next we show that the category $\mathbf{DMod}(G)$ of discrete G-modules also has enough injectives. As we indicated in Proposition 5.3.6, $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$ is the subcategory of $\mathbf{DMod}(G)$ consisting of those modules that are torsion.

Proposition 5.4.5 *Let G be a profinite group. Then* $\mathbf{DMod}(G)$ *has enough injectives, i.e., for every $A \in \mathbf{DMod}(G)$, there exists a monomorphism*

$$A \longrightarrow M_A$$

in $\mathbf{DMod}(G)$ *with M_A injective.*

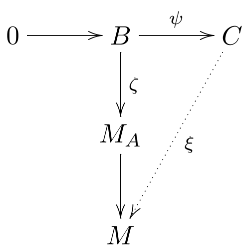
Proof. Denote by G_0 the abstract group underlying G. Let A be a discrete G-module; then obviously $A \in \mathbf{Mod}(G_0)$, the category of abstract G_0-modules. It is well known that $\mathbf{Mod}(G_0)$ has enough injectives (cf. Mac Lane [1963], page 93). Let

$$0 \longrightarrow A \xrightarrow{\varphi} M$$

be an exact sequence in $\mathbf{Mod}(G_0)$, with M injective in $\mathbf{Mod}(G_0)$. Define

$$M_A = \bigcup_U M^U,$$

where U runs through all open normal subgroups of G. Clearly $M_A \in \mathbf{DMod}(G)$. Let $a \in A$, and let U be an open normal subgroup of G such that $a \in A^U$. Then $\varphi(a) \in M^U$. Hence $\varphi(A) \subseteq M_A$. Finally M_A is injective in $\mathbf{DMod}(G)$ because any diagram



where ψ, ζ are mappings in $\mathbf{DMod}(G)$, with ψ a monomorphism, can be completed to a commutative diagram by a G_0-homomorphism $\xi : C \longrightarrow M$. However, since C is a discrete G-module, one has $\xi(C) \subseteq M_A$. □

Remark 5.4.6 The construction in the above proof can easily be modified to obtain enough injective objects in $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$ (respectively, in $\mathbf{DMod}([\![(\mathbf{Z}/n\mathbf{Z})G]\!])$, where n is a fixed natural number), by taking instead of M_A, its torsion G-submodule (respectively, the G-submodule of M_A consisting of those elements x such that $nx = 0$).

Exercise 5.4.7 Let Λ be a profinite ring.

(a) Assume that $P \in \mathbf{PMod}(\Lambda)$ is projective, i.e., that $\operatorname{Hom}_\Lambda(P, -)$ is exact as a functor on $\mathbf{PMod}(\Lambda)$. Prove that $\operatorname{Hom}_\Lambda(P, -)$ is also exact as a functor on the category $\mathbf{DMod}(\Lambda)$.
(b) Assume that $Q \in \mathbf{DMod}(\Lambda)$ is injective, i.e., that $\operatorname{Hom}_\Lambda(-, Q)$ is exact as a functor on $\mathbf{DMod}(\Lambda)$. Prove that $\operatorname{Hom}_\Lambda(-, Q)$ is also an exact as a functor on the category $\mathbf{PMod}(\Lambda)$. (Hint: use Lemma 5.1.4.)

5.5 Complete Tensor Products

Throughout this section R is a commutative profinite ring and Λ a *profinite R-algebra*, i.e., a profinite ring that contains a continuous homomorphic image of R in its center. Complete group rings $[\![RG]\!]$ are examples of profinite R-algebras. By abuse of notation we sometimes use the same symbol for an element $r \in R$ and for its image in Λ, when the homomorphism from R to Λ is an injection.

Let A be a profinite right Λ-module, B a profinite left Λ-module, and M an R-module. A continuous map

$$\varphi : A \times B \longrightarrow M$$

is called *middle linear* if $\varphi(a+a', b) = \varphi(a, b)+\varphi(a', b)$, $\varphi(a, b+b') = \varphi(a, b)+\varphi(a, b')$ and $\varphi(a\lambda, b) = \varphi(a, \lambda b)$ for all $a, a' \in A,\ b, b' \in B,\ \lambda \in \Lambda$.

We say that a profinite R-module T together with a middle linear map $A \times B \longrightarrow T$, denoted $(a, b) \mapsto a \mathbin{\widehat{\otimes}} b$, is a *complete tensor product* of A and B over Λ if the following universal property is satisfied: If M is a profinite R-module and $\varphi : A \times B \longrightarrow M$ a continuous middle linear map, then there exists a unique map of R-modules $\bar\varphi : T \longrightarrow M$ such that $\bar\varphi(a \mathbin{\widehat{\otimes}} b) = \varphi(a, b)$.

It is easy to see that if the complete tensor product exists, it is unique up to isomorphism. We denote it by $A \mathbin{\widehat{\otimes}}_\Lambda B$. Furthermore, it is clear that $\{a \mathbin{\widehat{\otimes}} b \mid a \in A, b \in B\}$ is a set of topological generators for the R-module $A \mathbin{\widehat{\otimes}}_\Lambda B$.

Note that it suffices to check the above universal property only for finite R-modules M, since every R-module is the inverse limit of its finite R-quotient modules.

Lemma 5.5.1 *With the above notation, the complete tensor product $A \mathbin{\widehat{\otimes}}_\Lambda B$ exists. In fact, if*

$$A = \varprojlim_{i \in I} A_i \quad \text{and} \quad B = \varprojlim_{j \in J} B_j,$$

where each A_i (respectively, B_i) is a finite right (respectively, left) Λ-module, then

$$A \mathbin{\widehat{\otimes}}_\Lambda B = \varprojlim_{i \in I, j \in J} (A_i \otimes_\Lambda B_j),$$

where $A_i \otimes_\Lambda B_j$ is the usual tensor product as abstract Λ-modules. In particular, $A \mathbin{\widehat{\otimes}}_\Lambda B$ is the completion of $A \otimes_\Lambda B$, where $A \otimes_\Lambda B$ has the topology for which a fundamental system of neighborhoods of 0 are the kernels of the natural maps

$$A \otimes_\Lambda B \longrightarrow A_i \otimes_\Lambda B_j \quad (i \in I, j \in J).$$

Proof. Observe that

$$A \times B = \varprojlim_{i \in I, j \in J} (A_i \times B_j).$$

It easily follows that there exists a canonical middle linear map

$$\iota : A \times B \longrightarrow \varprojlim_{i\in I, j\in J} (A_i \otimes_\Lambda B_j),$$

namely, the inverse limit of the canonical middle linear maps $A_i \times B_j \longrightarrow A_i \otimes B_j$. For $a \in A$, $b \in B$, put $a \widehat{\otimes} b = \iota(a,b)$. Let M be a finite Λ-module and $\varphi : A \times B \longrightarrow M$ a middle linear map. Since M is finite, there exist a pair of indices i, j such that φ factors through a map $\varphi_{ij} : A_i \times B_j \longrightarrow M$, which is also middle linear (this follows from an analog of Lemma 1.1.16). By the universal property of $A_i \otimes_\Lambda B_j$, there is an R-homomorphism $\bar{\varphi}_{ij} : A_i \otimes_\Lambda B_j \longrightarrow M$ such that $\bar{\varphi}_{ij}(a_i \otimes b_j) = \varphi_{ij}(a_i \times b_j)$ $(a_i \in A_i, b_j \in B_j)$. Define $\bar{\varphi} : A \widehat{\otimes}_\Lambda B \longrightarrow M$ as the composition $A \widehat{\otimes}_\Lambda B \longrightarrow A_i \otimes B_j \xrightarrow{\bar{\varphi}_{ij}} M$. Then $\bar{\varphi}\iota = \varphi$, as needed. □

A similar argument shows that "complete tensoring commutes with $\varprojlim$". More precisely,

Lemma 5.5.2 *Let*

$$\varprojlim_{i\in I} A_i \quad \text{and} \quad B = \varprojlim_{j\in J} B_j$$

be inverse limits of profinite right Λ-modules A_i and profinite left Λ-modules B_j, respectively. Then

$$\Big(\varprojlim_{i\in I} A_i\Big) \widehat{\otimes}_\Lambda \Big(\varprojlim_{j\in J} B_j\Big) = \varprojlim_{i\in I, j\in J} (A_i \widehat{\otimes}_\Lambda B_j).$$

The complete tensor product enjoys most of the properties of the usual tensor product of modules over abstract rings. If A is a profinite right Λ-module and $\rho : B \longrightarrow B'$ a continuous homomorphism of profinite left Λ-modules, define $A \widehat{\otimes}_\Lambda \rho : A \widehat{\otimes}_\Lambda B \longrightarrow A \widehat{\otimes}_\Lambda B'$ as the continuous R-homomorphism lifting the continuous middle linear map $A \times B \longrightarrow A \widehat{\otimes}_\Lambda B'$ given by $(a,b) \mapsto a \widehat{\otimes} \rho(a)$ $(a \in A, b \in B)$. If ρ is the identity, then obviously so is $A \widehat{\otimes}_\Lambda \rho$. It is clear that if $B \xrightarrow{\rho} B' \xrightarrow{\rho'} B''$, then $A \widehat{\otimes}_\Lambda (\rho\rho') = (A \widehat{\otimes}_\Lambda \rho)(A \widehat{\otimes}_\Lambda \rho')$. In other words, $A \widehat{\otimes}_\Lambda$—is a covariant functor. Similarly, if B is a profinite left Λ-module, $-\widehat{\otimes}_\Lambda B$ is a covariant functor. We record this as part of the following proposition.

Proposition 5.5.3 *Let R be a commutative profinite ring, Λ a profinite R-algebra, A a profinite right Λ-module, and B a profinite left Λ-module. Then*

(a) *$A \widehat{\otimes}_\Lambda$—is a right exact covariant functor.*
(b) *The functor $A \widehat{\otimes}_\Lambda$—is additive, that is, if B_1 and B_2 are profinite left Λ-modules, then there is a natural isomorphism of profinite R-modules,*

$$A \widehat{\otimes}_\Lambda (B_1 \oplus B_2) \cong A \widehat{\otimes}_\Lambda B_1 \oplus A \widehat{\otimes}_\Lambda B_2.$$

(c) *There is a natural isomorphism of profinite Λ-modules* $A \widehat{\otimes}_\Lambda \Lambda \cong A$.
(d) *If B is a finitely generated profinite left Λ-module, then*

$$A \widehat{\otimes}_\Lambda B = A \otimes_\Lambda B.$$

(e) *If A is a projective profinite right Λ-module, then the functor $A \widehat{\otimes}_\Lambda$—is exact.*
(f) *Similar statements for* $-\widehat{\otimes}_\Lambda B$.

Proof. (a) We have already seen that $A \widehat{\otimes}_\Lambda$—is a covariant functor. To show that this functor is right exact, we must prove that if

$$0 \longrightarrow B_1 \longrightarrow B_2 \xrightarrow{\varphi} B_3 \longrightarrow 0$$

is an exact sequence of profinite left Λ-modules, then

$$A \widehat{\otimes}_\Lambda B_1 \longrightarrow A \widehat{\otimes}_\Lambda B_2 \longrightarrow A \widehat{\otimes}_\Lambda B_3 \longrightarrow 0 \tag{3}$$

is an exact sequence of profinite R-modules. To see this, let $\{U_i \mid i \in I\}$ be the collection of all open Λ-submodules of B_2, and consider the inverse system of the exact sequences

$$0 \longrightarrow B_1/\rho^{-1}(U_i) \longrightarrow B_2/U_i \xrightarrow{\varphi} B_3/\varphi(U_i) \longrightarrow 0$$

of finite Λ-modules. Express A as an inverse limit $A = \varprojlim_{j \in J} A_j$ of finite Λ-modules. It is well-known (cf. Mac Lane [1963], page 148) that $A \otimes_\Lambda$—is right exact; hence

$$A_j \otimes_\Lambda B_1/\rho^{-1}(U_i) \longrightarrow A_j \otimes_\Lambda B_2/U_i \xrightarrow{\varphi} A_j \otimes_\Lambda B_3/\varphi(U_i) \longrightarrow 0$$

is exact for each $i \in I$. These sequences form an inverse system whose inverse limit is the sequence (3). Since $\varprojlim$ is an exact functor on the category of compact R-modules (analogous to Proposition 2.2.4), we deduce that (3) is exact.

We leave the proof of (b) and (c) to the reader. To prove (d), let A be a profinite right Λ-module generated by n elements and consider an epimorphism of profinite Λ-modules $\pi : \Lambda^n \longrightarrow A$, where Λ^n denotes the direct sum of n copies of Λ. By (b) and (c), $\Lambda^n \widehat{\otimes}_\Lambda B = \Lambda^n \otimes_\Lambda B$, so that $\Lambda^n \otimes_\Lambda B$ is compact. Now, π induces an epimorphism $\Lambda^n \otimes_\Lambda B \longrightarrow A \otimes_\Lambda B$. Since $A \otimes_\Lambda B$ is dense in $A \widehat{\otimes}_\Lambda B$ and this epimorphism is continuous, one deduces that $A \otimes_\Lambda B$ is compact as well. Thus $A \widehat{\otimes} B = A \otimes_\Lambda B$.

Finally we show (e). Since A is projective, there exists a free Λ-module $[\![\Lambda X]\!]$ on some profinite space X such that A is a direct summand of $[\![\Lambda X]\!]$ by Lemma 5.5.2. From property (b) (applied to $-\widehat{\otimes}_\Lambda B$) one sees that it suffices to show that the functor $[\![\Lambda X]\!] \widehat{\otimes}_\Lambda$—is exact. Write $[\![\Lambda X]\!] = \varprojlim [\![\Lambda X_i]\!]$, where each X_i is finite. Since $\varprojlim$ is exact, we are reduced to the case when X is finite. Then, the result follows immediately from properties analogous to (b) and (c). □

Let Λ and Δ be profinite R-algebras, and let B be a profinite Δ-Λ *bimodule*, that is, a profinite left Δ-module which is at the same time a profinite right Λ-module such that for each $b \in B, \delta \in \Delta, \lambda \in \Lambda$ and $r \in R$, one has $(\delta b)\lambda = \delta(b\lambda)$ and $rb = br$. Assume that A is a profinite left Λ-module, D a profinite right Δ-module and C is a discrete left Δ-module. Then one easily proves the following

Proposition 5.5.4

(a) $B \widehat{\otimes}_\Lambda A$ *is a profinite left* Δ*-module, with an action determined by*

$$\delta(b \widehat{\otimes}_\Lambda a) = \delta b \widehat{\otimes}_\Lambda a \quad (\delta \in \Delta,\ a \in A,\ b \in B).$$

(b) $\mathrm{Hom}_\Delta(B, C)$ *is a discrete left* Λ*-module, with action determined by*

$$(\lambda\varphi)(b) = \varphi(b\lambda) \quad (\lambda \in \Lambda,\ b \in B,\ \varphi \in \mathrm{Hom}_\Delta(B, C)).$$

(c) *There is a unique natural isomorphism of discrete* R*-modules*

$$\Phi : \mathrm{Hom}_\Lambda(A, \mathrm{Hom}_\Delta(B, C)) \longrightarrow \mathrm{Hom}_\Delta(B \widehat{\otimes}_\Lambda A, C)$$

such that

$$\Phi(\varphi)(b \widehat{\otimes} a) = \varphi(a)(b) \quad (a \in A,\ b \in B,\ \varphi \in \mathrm{Hom}_\Lambda(A, \mathrm{Hom}_\Delta(B, C))).$$

(d) $D \widehat{\otimes}_\Delta (B \widehat{\otimes}_\Lambda A) \cong (D \widehat{\otimes}_\Delta B) \widehat{\otimes}_\Lambda A.$

Exercise 5.5.5 Let R be a commutative profinite ring.

(a) Let X and Y be profinite spaces. Then $[\![R(X \times Y)]\!] \cong [\![RX]\!] \widehat{\otimes}_R [\![RY]\!]$ as R-modules.
(b) Let G and H be profinite groups. Then $[\![R(G \times H)]\!] \cong [\![RG]\!] \widehat{\otimes}_R [\![RH]\!]$ as R-algebras.

5.6 Profinite G-spaces

Let G be a profinite group and X a topological space. We say that X is a *left G-space*, or simply a *G-space* if there exists a continuous map

$$G \times X \to X,$$

denoted $(g, x) \mapsto gx$, such that $(gh)x = g(hx)$ and $1x = x$ for all $g, h \in G$, $x \in X$ (one says then that G *operates* or *acts* on X on the left). A pointed topological space $(X, *)$ is a G-space if X is a G-space in the above sense, and in addition $g* = *$ for all $g \in G$. There are corresponding notions of right G-spaces or pointed right G-spaces. Note that G-modules are examples of pointed G-spaces.

Remark 5.6.1

(1) If X is a G-space, then for each $g \in G$, the map $\alpha_g : X \longrightarrow X$ defined by $x \mapsto gx$ is easily seen to be a homeomorphism of X to X; moreover the map

$$\alpha : G \longrightarrow \mathrm{Homeo}(X)$$

given by $\alpha \mapsto \alpha_g$ is a homomorphism of G to the group of homeomorphisms $\mathrm{Homeo}(X)$ of X. If one imposes the compact-open topology on $\mathrm{Homeo}(X)$, one can prove that the homomorphism α is continuous if an only if G operates on X continuously (cf. Bourbaki [1989], X, 3.4, Theorem 3).

(2) Similarly, if A is a G-module, then for each $g \in G$, the map $\alpha_g : A \longrightarrow A$ defined by $a \mapsto ga$ is a continuous automorphism of the topological group A; moreover the map

$$\alpha : G \longrightarrow \mathrm{Aut}(A)$$

given by $\alpha \mapsto \alpha_g$ is a homomorphism of groups. If one imposes the compact-open topology on $\mathrm{Aut}(A)$, one can use the result in Bourbaki just mentioned to prove that the homomorphism α is continuous if an only if G operates on A continuously.

Exercise 5.6.2 Let G and H be abstract groups. Recall that G is said to *operate* or *act* on H (as groups) if there is an action

$$G \times H \longrightarrow H,$$

which we denote by $(g, h) \mapsto \alpha_g(h)$ $(g \in G, h \in H)$, of G on H such that for each $g \in G$, the map $\alpha_g : H \longrightarrow H$ is an automorphism of H.

(a) Let G and H be profinite groups. Prove that G operates on H continuously if and only if there is a continuous homomorphism

$$G \longrightarrow \mathrm{Aut}(H)$$

from G to the group of continuous automorphisms of H, where $\mathrm{Aut}(H)$ is endowed with the compact-open topology. (Hint: use the result in Bourbaki mentioned in Remark 5.6.1.)

(b) Let G and H be topological groups. Assume that G acts on H continuously. Endow the corresponding semidirect product $H \rtimes G$ with the product topology (recall that $H \rtimes G$ can be identified with $H \times G$, as sets). Prove that then $H \rtimes G$ is a topological group.

(c) Let $\mathcal{C}$ be an NE-formation of finite groups (see Section 2.1). Prove that if G and H are pro-$\mathcal{C}$ groups and G acts continuously on H, then the semidirect product $H \rtimes G$ determined by this action is a pro-$\mathcal{C}$ group.

(d) Let $F = F_{\mathcal{C}}(X)$ (respectively, $F = F_{\mathcal{C}}(X, *)$) be a free pro-$\mathcal{C}$ group on a profinite space X (respectively, on a pointed profinite space $(X, *)$) and let G be a profinite group. Assume that G acts continuously on X (respectively, on $(X, *)$). Prove that this action extends uniquely to a continuous action of the group G on the group F.

If X and Y are G-spaces, a *G-map* $\varphi : X \longrightarrow Y$ is a continuous map such that $\varphi(gx) = g\varphi(x)$ $(g \in G, x \in X)$. If the spaces are pointed, we require in addition that $\varphi(*) = *$. G-spaces and their maps form a category; similarly, pointed G-spaces and their maps form a category.

Let X be a profinite G-space; we say that decomposition $X = \varprojlim X_i$, as an inverse limit of spaces, is a *G-decomposition* if this is an inverse limit in the category of profinite G-spaces, that is, if each X_i is a profinite G-space and the canonical maps $X_i \longrightarrow X_j$ are G-maps. There is an analogous concept of G-decomposition for pointed profinite G-spaces.

Let G be a profinite group and X a G-space. We denote the *quotient space* under this action by $G\backslash X$: it is the space of the *G-orbits* $Gx = \{gx \mid g \in G\}$ of each $x \in X$. If the action of G on X is on the right, we denote the quotient by X/G, and the orbits by xG. There is a natural onto map $G \longrightarrow G\backslash X$ that sends each $x \in X$ to its G-orbit. The topology of $G\backslash X$ is the quotient topology.

The following lemma is an immediate consequence of continuity of the action and of compactness.

Lemma 5.6.3 *Let G be a profinite group and let X be a Hausdorff G-space.*

(a) *Assume that $x \in X$. Then the G-stabilizer $G_x = \{g \in G \mid gx = x\}$ of x is closed in G.*
(b) *If X is profinite, so is $G\backslash X$.*

The action of G on X (respectively, on $(X, *)$) is called *free* if $G_x = 1$ of each $x \in X$ (respectively, $G_x = 1$ for all $x \neq *$ in X). One also uses the expressions "G acts freely" or "X or $(X, *)$ is a free G-space".

Recall that a topological space is countably based (see Section 1.1) if it has a countable base of open subsets.

Lemma 5.6.4 *Let G be a profinite group acting on a profinite space X (respectively, a pointed profinite space $(X, *)$). Then*

(a) *X (respectively, $(X, *)$) admits a G-decomposition as an inverse limit of finite quotient G-spaces*

$$X = \varprojlim_{i \in I} X_i \quad \Big(\text{respectively, } (X, *) = \varprojlim_{i \in I} (X_i, *)\Big).$$

(b) *Suppose that G is finite and acts freely on X. If*

$$X = \varprojlim_{i \in I} X_i$$

is as in (a), *then there exists some $i_o \in I$ such that G acts freely on X_j for every $j \succeq i_0$; in particular, X admits a decomposition as an inverse limit of finite quotient free G-spaces.*

(c) *Suppose that G is finite and acts freely on a pointed profinite space $(X, *)$. Then there exists a G-decomposition of $(X, *)$ as an inverse limit of finite quotient free G-spaces*

$$(X, *) = \varprojlim_{i \in I} (X_i, *).$$

(d) *If X is countably based, the poset $(I, \succeq)$ in parts* (a), (b) *and* (c) *can be chosen to be countable and totally ordered.*

Proof. (a) We consider here the nonpointed case. For the pointed case, the proof is similar. First we show that for any open equivalence relation R on X, there exists a G-invariant open equivalence relation $S \subseteq R$. Indeed, consider R as a subset of $X \times X$ on which G acts coordinatewise. Observe that if $g \in G$, then gR is also an open equivalence relation on X. Set

$$S = \bigcap_{g \in G} gR.$$

Clearly S is a G-invariant equivalence relation on X. Let us prove that S is open. Fix $s \in S$. Then for all $g \in G$, $gs \in R$. Since the action of G on $X \times X$ is continuous, for every $g \in G$ there exist open neighborhoods V_g, W_g of the points g and s, respectively, such that $V_g W_g \subseteq R$. The set $\{V_g \mid g \in G\}$ is an open covering of G. By the compactness of G, there exists a finite subcovering $V_{g_1}, \dots, V_{g_n}$ of G. Set

$$W_s = \bigcap_{i=1}^{n} W_{g_i}.$$

Then $gW_s \subseteq R$, for all $g \in G$. Therefore $W_s \subseteq S$ and W_s is an open neighborhood of s. Since this is true for all $s \in S$, then $S = \bigcup_{s \in S} W_s$ is open. This shows that the set of all G-invariant open equivalence relations on X is cofinal in the set of all open equivalence relations on X.

Thus (see the proof of (c) $\Rightarrow$ (a) in Theorem 1.1.12) it follows that $X = \varprojlim X/S$, where S runs through all G-invariant open equivalence relations on X, i.e., X is the inverse limit of finite G-spaces.

(b) Suppose that G is finite. Consider a G-decomposition $X = \varprojlim X_i$ as an inverse limit of finite G-spaces X_i. Denote by S_i the subset of G of all $g \neq 1$ such that $gx = x$ for some $x \in X_i$. We claim that $\bigcap_i S_i = \emptyset$. Assume not; then, for $g \in \bigcap_i S_i$, the sets $Y_i^g = \{x \in X_i \mid gx = x\}$ are finite, nonempty and form a natural inverse system. So, the limit $Y^g = \varprojlim Y_i^g$ is not empty (see Proposition 1.1.4), and $gx = x$ for any $x \in Y^g$. This contradicts the freeness of the action of G on X, and hence the claim is proved. Note that if

$j \preceq i$, then $S_i \subseteq S_j$. Since G is finite there exists i_0 such that $S_i = \emptyset$ (i.e., G acts freely on X_j) for any $i \succeq i_0$. Therefore,

$$X = \varprojlim_{j \succeq i_0} X_j$$

is a decomposition of the desired form.

(c) It follows from part (a) that $(X, *)$ can be written as

$$(X, *) = \varprojlim_{i \in I} (X_i, *),$$

where $\{(X_i, *), \psi_{ij}\}$ is the inverse system of all finite pointed quotient G-spaces of $(X, *)$. Fix an index $j \in I$. We need to prove that there exists an index $j' \in I$ such that $j' \succeq j$ and $(X_{j'}, *)$ is a pointed free G-space; observe that to do this we simply have to exhibit a finite pointed free G-space $(Z, *)$ together with G-epimorphisms of pointed spaces $\mu : (X, *) \longrightarrow (Z, *)$ and $\nu : (Z, *) \longrightarrow (X_j, *)$ such that $\nu\mu = \psi_j$, where $\psi_j : (X, *) \longrightarrow (X_j, *)$ is the canonical projection.

Set $X' = X - \psi_j^{-1}(*)$. We claim that X' is a G-subspace. Indeed, if $g \in G$, $x \in X'$ and we had $gx \notin X'$, then $g\psi_j(x) = \psi_j(gx) = *$; hence $\psi_j(x) = *$, contradicting our choice of x. Therefore, X' is a free G-space. Then

$$X' = \varprojlim_{i \succeq j} \psi_i(X')$$

is a G-decomposition of X'. By part (b), there exists some $i_0 \in I$ with $i_0 \succeq j$ such that $\psi_{i_0}(X')$ is a finite free G-space. Define $Z = \psi_{i_0}(X') \,\dot\cup\, \{*\}$. Then $(Z, *)$ is in a natural way a finite pointed free G-space. Define

$$\mu : (X, *) \longrightarrow (Z, *)$$

by

$$\mu(x) = \begin{cases} \psi_{i_0}(x), & \text{if } x \in X'; \\ *, & \text{if } x \in \psi_j^{-1}(*), \end{cases}$$

and define $\nu : (Z, *) \longrightarrow (X_j, *)$ by

$$\nu(x) = \begin{cases} \psi_{i_0 j}(x), & \text{if } x \in \psi_{i_0}(X'); \\ *, & \text{if } x = * \,. \end{cases}$$

Clearly μ and ν satisfy the required conditions.

(d) This follows from Corollary 1.1.13. □

Let G be a profinite group, X a G-space and $\pi : X \to G\backslash X$ the canonical quotient map. We say that π admits a continuous section if there exists a continuous map $\sigma : G\backslash X \to X$ such that $\pi\sigma = \mathrm{id}_{G\backslash X}$. In other words, there exists a closed subspace Z of X such that the restriction $\pi_{|Z}$ of π to Z is a homeomorphism onto $G\backslash X$.

Lemma 5.6.5 *Let G be a profinite group acting freely on a profinite space X, and let*

$$\pi : X \to G\backslash X$$

denote the canonical quotient map. Then

(a) *There exists a continuous section $\sigma : G\backslash X \to X$ of π;*
(b) *If Y is a closed subset of X such that $\pi_{|Y}$ is injective, then σ can be chosen such that Y is a subset of $\sigma(G\backslash X)$.*

Proof. (a) Assume first that G finite. By Lemma 5.6.4(b), there exists a finite G-quotient space X_0 of X, on which G acts freely. Let $\varphi_0 : X_0 \longrightarrow G\backslash X_0$ be the canonical quotient map. Choose $Z_0 \subseteq X_0$ to be such that the restriction of φ_0 to Z_0 is bijective. Denote by $\pi_0 : X \longrightarrow X_0$ the natural G-epimorphism. Then $Z = \pi_0^{-1}(Z_0)$ is the desired subset. Indeed, since Z is compact, it suffices to check that $\varphi_{|Z}$ is injective and surjective, and these properties follow easily since G acts freely on both X and X_0.

Now let G be infinite. We proceed in a way similar to the proof of Proposition 2.2.2. Let $\mathcal{L}$ be the set of all closed normal subgroups of G. For $L \in \mathcal{L}$, put $X_L = L\backslash X$. Then G/L acts freely on X_L. Consider the collection $\mathcal{P}$ of all closed subspaces Z_L of X_L ($L \in \mathcal{L}$) such that the restriction of the canonical epimorphism

$$\varphi_L : X_L \longrightarrow (G/L)\backslash X_L = G\backslash X$$

to Z_L is a homeomorphism. Define a partial ordering on $\mathcal{P}$ by $Z_L \preceq Z_K$ if $K \leq L$ and $Z_L = \pi_{KL}(Z_K)$, where π_{KL} is the natural projection $X_K \to X_L$. Then $\mathcal{P}$ is an inductive poset: if $\{Z_{M_i} \mid i \in I\}$ is a linearly ordered subset of $\mathcal{P}$, set $M_0 = \bigcap_{i\in I} M_i$ and $Z_{M_0} = \varprojlim_{i\in I} Z_{M_i}$; one verifies without difficulty that Z_{M_0} is in $\mathcal{P}$ and that it is an upper bound for $\{Z_{M_i} \mid i \in I\}$. Zorn's Lemma provides a maximal element Z_M in $\mathcal{P}$. It suffices to prove that $M = 1$. Suppose $M \neq 1$. Then there is some normal subgroup L of G such that $L < M$ and M/L is finite. Note that $(M/L)\backslash X_L = X_M$. Now we use the finite case considered above to obtain a closed subspace Z'_L of X_L such that the restriction of the natural epimorphism $\varphi_{LM} : X_L \to X_M$ to Z'_L is a homeomorphism. Define $Z_L = Z'_L \cap \varphi_{LM}^{-1}(Z_M)$. Then $(Z_L, *) \in \mathcal{P}$ and $Z_L \succ Z_M$, contradicting the maximality of Z_M.

(b) Define an equivalence relation on X by setting $x \sim y$ if and only if either $x, y \in gY$ for some $g \in G$, or $x = y$. The quotient space X_0 of X modulo this equivalence relation is a profinite space with induced free action of G. By (a), there is a closed subset Z_0 of X_0 mapping bijectively onto $G\backslash X_0$. The desired subset Z is the preimage of X_0 in X. $\square$

Corollary 5.6.6 *Let G act freely on the profinite space X and let*

$$\pi : X \longrightarrow G\backslash X$$

be the canonical projection. Choose a continuous section σ of π and define $Z = \sigma(G\backslash X)$. Then the map $\rho : G \times Z \longrightarrow X$ given by $(g, z) \mapsto gz$ ($g \in G$, $z \in Z$) is a homeomorphism. This is a map of G-spaces, where the G-structure of $G \times Z$ is defined by multiplication on the first component.

Proof. Clearly ρ is a bijective G-map; furthermore ρ is continuous since it is the restriction of the action map $G \times X \longrightarrow X$, which is continuous by assumption. Since $G \times Z$ is compact, ρ is a homeomorphism. □

Lemma 5.6.7 *Let G be a profinite group and let X be a second countable profinite G-space, i.e., $w(X) = \aleph_0$. Then the quotient map $\pi : X \longrightarrow G\backslash X$ admits a continuous section $\sigma : G\backslash X \longrightarrow X$. More generally, suppose that Y is a closed subset of X such that $\pi_{|Y}$ is injective; then σ can be chosen such that Y is a subset of $\sigma(G\backslash X)$.*

Proof. We shall prove the second statement. Denote by $\tilde{\sigma} : \pi(Y) \longrightarrow Y$ the (continuous!) inverse of $\pi_{|Y}$. We need a continuous section σ of π extending $\tilde{\sigma}$.

According to Lemma 5.6.4(a), if $\mathcal{S}$ is the collection of all G-invariant open equivalence relations S on X, then

$$X = \varprojlim_{S \in \mathcal{S}} X/S$$

(see the proof of that lemma for this viewpoint).

First we show, with no conditions on $w(X)$, that given $S \in \mathcal{S}$ there exists a G-invariant open equivalence relation R on X with $R \leq S$ and such that

$$y_1, y_2 \in Y \quad \text{and} \quad y_1 R(gy_2) \quad (\text{some } g \in G) \quad \Longrightarrow \quad y_1 R y_2. \qquad (4)$$

Consider first the equivalence relation S_Y induced by S on Y: $S_Y = (Y \times Y) \cap S$. Then S_Y is an open equivalence relation on Y. Since Y is compact, $\pi_{|Y} : Y \longrightarrow \pi(Y)$ is a homeomorphism, hence $\tilde{S}_Y = (\pi \times \pi)(S_Y)$ is an open equivalence relation on $\pi(Y)$. Since $\pi(Y)$ is compact, there exists an open equivalence relation $\tilde{T}$ on $G\backslash X$ whose restriction to $\pi(Y)$ is $\tilde{S}_Y$. Define $T = (\pi \times \pi)^{-1}(\tilde{T})$; then T an open G-invariant equivalence relation on X. Define

$$R = S \cap T.$$

Then R is clearly a G-invariant open equivalence relation on X, and $R \leq S$. Furthermore, if $y_1, y_2 \in Y$ and $y_1 R(gy_2)$, for some $g \in G$, then $\pi(y_1)\tilde{T}\pi(gy_2)$, and hence $\pi(y_1)\tilde{T}\pi(y_2)$, i.e., $y_1 T y_2$. On the other hand, since $y_1, y_2 \in Y$, $\pi(y_1)\tilde{T}\pi(y_2)$ also means that $\pi(y_1)\tilde{S}_Y\pi(y_2)$, and so $y_1 S_Y y_2$, i.e., $y_1 S y_2$. Thus $y_1 R y_2$.

Let $\mathcal{R}$ is the collection of all open G-invariant equivalence relation on X satisfying condition (4). Then we have proved that $\mathcal{R}$ is cofinal in $\mathcal{S}$, and so

$$X = \varprojlim_{R \in \mathcal{R}} X/R.$$

For $R \in \mathcal{R}$, let Y_R denote the canonical image of Y in the finite G-space $X_R = X/R$, and let $\pi_R : X_R \longrightarrow G\backslash X_R$ denote the canonical projection. Then

$$\pi = \varprojlim_{R \in \mathcal{R}} \pi_R;$$

furthermore, by condition (4), π_R is an injection when restricted to Y_R $(R \in \mathcal{R})$.

Next we use the assumption that X is second countable to construct compatible sections $\sigma_R : G\backslash X_R \longrightarrow X_R$ of $\pi_{|R}$ $(R \in \mathcal{R})$. Since X is second countable, $\mathcal{R}$ is countable. We may replace $\mathcal{R}$ by a cofinal subset $\mathcal{R}'$ that is totally ordered: $\mathcal{R}' = \{R'_1, R'_2, \ldots\}$, where $R'_1 \geq R'_2 \geq \cdots$ (if $\mathcal{R} = \{R_1, R_2, \ldots\}$, define $R'_1 = R_1$, and recursively, $R'_{n+1} = R'_n \cap R_{n+1}$). For each $n \in \mathbf{N}$, put $X_n = X_{R'_n}$, $Y_n = Y_{R'_n}$ and $\pi_n = \pi_{R'_n}$. Denote by $\tilde{\sigma}_n : \pi_n(Y_n) \longrightarrow Y_n$ the unique map such that $\pi_n \tilde{\sigma}_n = \mathrm{id}_{\pi_n(Y_n)}$. Choose an arbitrary section

$$\sigma_1 : G\backslash X_1 \longrightarrow X_1$$

of π_1 such that σ_1 extends $\tilde{\sigma}_1$. Assuming that compatible sections

$$\sigma_i : G\backslash X_i \longrightarrow X_i$$

$(1 = 1, \ldots, n)$ have been chosen, construct a section

$$\sigma_{n+1} : G\backslash X_{n+1} \longrightarrow X_{n+1}$$

extending $\tilde{\sigma}_{n+1}$ such that the diagram

$$\begin{array}{ccc} X_{n+1} & \underset{\sigma_{n+1}}{\overset{\pi_{n+1}}{\rightleftarrows}} & G\backslash X_{n+1} \\ \downarrow & & \downarrow \\ X_n & \underset{\sigma_n}{\overset{\pi_n}{\rightleftarrows}} & G\backslash X_n \end{array}$$

commutes. Define

$$\sigma = \varprojlim_{n \in \mathbf{N}} \sigma_n.$$

Then $\sigma : G\backslash X \longrightarrow X$ is a continuous section of π extending

$$\varprojlim_{n \in \mathbf{N}} \tilde{\sigma}_n = \tilde{\sigma}.$$

So, $\sigma(G\backslash X)$ contains $\varprojlim_{n \in \mathbf{N}} \tilde{\sigma}_n(G\backslash X_n) = Y$. $\square$

Next example shows that the assumptions of Lemmas 5.6.5 and 5.6.7 cannot be avoided.

Example 5.6.8 We construct a profinite G-space X such that the quotient map

$$\pi : X \longrightarrow G\backslash X$$

does not have a continuous section.

Let $K = \{0, 1, -1\}$ be the field of integers modulo 3 with the discrete topology, and let $G = \{1, -1\}$ be the multiplicative group of K. Let I be an indexing set, and consider the direct product

$$X = \prod_I K$$

of copies of K (as a discrete space) indexed by I. Then X is a profinite space on which G operates continuously in a natural way. Let $\pi : X \longrightarrow G\backslash X$ be the canonical quotient map. We shall prove that π admits a continuous section if and only if I is countable. By Lemma 5.6.7, π admits a continuous section if I is countable.

Conversely, assume that $\sigma : G\backslash X \longrightarrow X$ is a continuous section of π and let $Z = \mathrm{Im}(\sigma)$. Hence Z is a compact subset of X such that $0 \in Z$ and if $0 \neq x \in X$, then either $1 \in Z$ or $-1 \in Z$ (not both). Let J be a finite subset of I and let $u = (u_i) \in X$ be such that $u_i = 0$ for $i \notin J$. Define

$$B(J, u) = \left\{ x \in \prod_I K \mid x_j = u_j \text{ for all } j \in J \right\}.$$

Then the subsets of X of the form $B(J, u)$ are clopen and constitute a base for the topology of X. For $i \in I$, write e_i for the element of X which has entry 1 at position i and entry 0 elsewhere. Define $\epsilon_i \in \{1, -1\}$ to be such that $\epsilon_i e_i \notin Z$. Since Z is closed, for each $i \in I$ there exists a finite subset J_i of I such that $i \in J_i$ and $B(J_i, \epsilon_i e_i) \cap Z = \emptyset$.

Consider now any two distinct indices $i, j \in I$. We claim that either $i \in J_j$ or $j \in J_i$ (or both). To see this, set $x = \epsilon_i e_i - \epsilon_j e_j$. Assume that $i \notin J_j$ and $j \notin J_i$. Then, $x \notin Z$ (since $j \notin J_i$ implies $x \in B(J_i, \epsilon_i e_i)$); similarly, $-x \notin Z$ (since $i \notin J_j$ implies $x \in B(J_j, \epsilon_j e_j)$). This is a contradiction, and so the claim is proved.

Next we show that I is countable. Let N be a countably infinite subset of I and set $P = \bigcup_{i \in N} J_i$. If I were uncountable, there would be some $j \in I - P$, since P is countable. Then, by construction, $j \notin J_i$, for any $i \in N$. Therefore, $i \in J_j$ by the preceding paragraph. In particular, $N \subseteq J_j$, contradicting the finiteness of J_j.

Exercise 5.6.9

(a) Extend the example above to a finite group G acting on a profinite space $X = \prod_I (G \cup \{*\})$, with an appropriate action of G on the discrete space $G \cup \{*\}$, and where I is an uncountable indexing set.

(b) Extend Example 5.6.8 to any profinite group G. Namely, prove that given a profinite group G, there is a profinite space G-space X such that the canonical map $X \longrightarrow G\backslash X$ does not admit a continuous section.
(c) Use Example 5.6.8 to exhibit an example where Lemma 5.6.5(a) fails if one assumes that X is only locally compact.

5.7 Free Profinite $[\![RG]\!]$-modules

Let R be a commutative profinite ring, G a profinite group and X a profinite G-space. The action of G on X induces a natural action of the complete group ring $[\![RG]\!]$ on the free profinite R-module $[\![RX]\!]$; one can see this as follows. Express X as an inverse limit

$$X = \varprojlim_{i \in I} X_i$$

of finite G-spaces X_i (see Lemma 5.6.4(a)). For each $i \in I$, consider the open normal subgroup of G defined by $U_i = \bigcap_{x \in X_i} G_x$. For each $i \in I$ there is an obvious continuous action

$$[R(G/U_i)] \times [RX_i] \longrightarrow [RX_i]$$

of the ring $[R(G/U_i)]$ on the profinite abelian group $[RX_i]$. Hence there is a continuous action

$$[\![RG]\!] \times [RX_i] \longrightarrow [RX_i]$$

of the ring $[\![RG]\!]$ on the profinite abelian group $[RX_i]$ induced by the continuous ring homomorphism $[\![RG]\!] \longrightarrow [R(G/U_i)]$. Taking inverse limits, we get the indicated action

$$[\![RG]\!] \times [\![RX]\!] \longrightarrow [\![RX]\!].$$

One has similar definitions for pointed spaces.

Proposition 5.7.1

(a) *Let a profinite group G act freely on a profinite space X. Then for any profinite commutative ring R, the module $[\![RX]\!]$ is a free $[\![RG]\!]$-module on the space $G\backslash X$.*
(b) *Conversely, every free profinite left $[\![RG]\!]$-module has the form $[\![R(G \times Z)]\!]$ for some profinite space Z, where the action of G on $G \times Z$ is by left multiplication on the first component.*

Proof. (a) By Corollary 5.6.6, there exists an isomorphism of G-spaces $G \times Z \cong X$, where Z is a certain closed subspace of X, and where the action of G on $G \times Z$ is by left multiplication on the first component. Write $Z = \varprojlim_{i \in I} Z_i$, where the Z_i are finite quotient spaces of Z. Let G act on $G \times Z_i$ by left multiplication on the first component. Correspondingly we have a decomposition

$$X = G \times Z = \varprojlim_{i \in I} (G \times Z_i),$$

as G-spaces. Now, since Z_i is finite, we have natural $[\![RG]\!]$-isomorphisms

$$[\![R(G \times Z_i)]\!] \cong \bigoplus_{z \in Z_i} [\![RG]\!] z.$$

Hence, for each $i \in I$, $[\![R(G \times Z_i)]\!]$ is a free $[\![RG]\!]$-module on the space Z_i. Taking limits we get the desired result.

(b) For the converse, observe that if a free $[\![RG]\!]$-module has a finite basis, say Y, then it has the form

$$\bigoplus_{y \in Y} [\![RG]\!] y \cong [\![R(G \times Y)]\!],$$

where the isomorphism is an $[\![RG]\!]$-module isomorphism. The case of a general profinite basis follows from this and from Lemma 5.6.4 by an inverse limit argument as in (a). □

Corollary 5.7.2 *Let R a commutative profinite ring and let H be a closed subgroup of a profinite group G. Then*

(a) *Every free $[\![RG]\!]$-module is a free $[\![RH]\!]$-module. In particular $[\![RG]\!]$ is a free $[\![RH]\!]$-module*;
(b) *Every projective profinite $[\![RG]\!]$-module is a projective $[\![RH]\!]$-module*;
(c) *Every injective discrete $[\![RG]\!]$-module is an injective $[\![RH]\!]$-module.*

Proof. Part (b) follows from (a) since a profinite projective module is a direct summand of a free module (see Proposition 5.4.2). To prove (a), let A be a free $[\![RG]\!]$-module. By Proposition 5.7.1, A has the form $[\![R(G \times Z)]\!]$. Then

$$A = [\![R(G \times Z)]\!] = [\![R(H \times (H \backslash G) \times Z)]\!].$$

Since the action of H on the basis $H \times (H \backslash G) \times Z$ is multiplication on H, it is a free action; hence, again by Proposition 5.7.1, A is a free H-module.

Part (c) is obtained from (b) by duality. □

5.8 Diagonal Actions

Let R be a commutative profinite ring and let G be a profinite group. Assume that A is a profinite left $[\![RG]\!]$-module and A' a discrete left $[\![RG]\!]$-module. Then $\mathrm{Hom}_R(A, A')$ is an R-module with the action $(rf)(a) = rf(a)$ $(r \in R, a \in A, f \in \mathrm{Hom}_R(A, A'))$. The *diagonal* action of G on $\mathrm{Hom}(A, A')$ is defined as follows: if $f \in \mathrm{Hom}_R(A, A')$ and $x \in G$, then xf is the R-homomorphism $A \longrightarrow A'$ given by

$$(xf)(a) = xf(x^{-1}a) \quad (a \in A).$$

Observe that $\mathrm{Hom}_R(A, A')$, with the compact-open topology, is discrete. It follows from the decomposition of Lemma 5.1.4 that the diagonal action is continuous, making $\mathrm{Hom}(A, A')$ into a discrete $[\![RG]\!]$-module.

Assume now that A and A' are profinite left $[\![RG]\!]$-modules. The diagonal action of G on the R-module $A \widehat{\otimes} A'$ is defined as follows: if $x \in G$, $a \in A$ and $a' \in A'$, set

$$x(a \widehat{\otimes} a') = (xa) \widehat{\otimes} (xa').$$

Using Lemma 5.5.1 one sees that this is a continuous action, making $A \widehat{\otimes} A'$ into a profinite left $[\![RG]\!]$-module.

Note that one has similar definitions of diagonal actions in the case that A and A' are not necessarily both *left* $[\![RG]\!]$-modules. For example, if A is a profinite right $[\![RG]\!]$-module and A' a discrete left $[\![RG]\!]$-module, then the diagonal action on $\mathrm{Hom}(A, A')$ is given by $(xf)(a) = xf(ax)$ $(x \in G, f \in \mathrm{Hom}(A, A'), a \in A)$. If A is a profinite right $[\![RG]\!]$-module and A' a profinite left $[\![RG]\!]$-module, then the diagonal action on $A \widehat{\otimes} A'$ is given by $x(a \widehat{\otimes} a') = (ax^{-1}) \widehat{\otimes} (xa')$ $(x \in G, a \in A, a' \in A')$.

Proposition 5.8.1 *Let $H \leq_c G$ be profinite groups, R a commutative profinite ring and B a right $[\![RG]\!]$-module. Then, there exists an isomorphism of right $[\![RG]\!]$-modules*

$$B \widehat{\otimes}_{[\![RH]\!]} [\![RG]\!] \cong B \widehat{\otimes}_R [\![R(H\backslash G)]\!],$$

where the action of $[\![RG]\!]$ on $B \widehat{\otimes}_{[\![RH]\!]} [\![RG]\!]$ is via the right action on $[\![RG]\!]$, and its action on $B \widehat{\otimes}_R [\![R(H\backslash G)]\!]$ is the diagonal action.

Proof. Define a map

$$\varphi : B \times G \longrightarrow B \widehat{\otimes}_R [\![R(H\backslash G)]\!]$$

by $\varphi(b, g) = bg \widehat{\otimes} Hg$, $(b \in B, g \in G)$. Note that φ is middle H-linear, i.e., $\varphi(bh, g) = \varphi(b, hg)$, for all $h \in H$. Moreover, φ is continuous, for it is the inverse limit of maps of finite sets

$$B/BU \times G/U \longrightarrow B/BU \widehat{\otimes}_R [\![R(HU\backslash G)]\!],$$

where U ranges over the open normal subgroups of G. Hence φ induces a continuous homomorphism

$$\varphi : B \widehat{\otimes}_{[\![RH]\!]} [\![RG]\!] \longrightarrow B \widehat{\otimes}_R [\![R(H\backslash G)]\!].$$

One easily checks that this homomorphism has an inverse homomorphism ψ determined by $\psi(b \widehat{\otimes} Hg) = bg^{-1} \widehat{\otimes} g$ $(b \in B, g \in G)$. $\square$

Corollary 5.8.2 *Let G, R and B be as above. Denote by B_0 the underlying R-module of B (i.e., we forget the G-module structure of B). Then there is an isomorphism of right $[\![RG]\!]$-modules*

$$B_0 \widehat{\otimes}_R [\![RG]\!] \cong B \widehat{\otimes}_R [\![RG]\!],$$

given by $b \widehat{\otimes} g \mapsto bg \widehat{\otimes} g$ ($[\![RG]\!]$ acts on $B \widehat{\otimes}_R [\![RG]\!]$ via its right action on $[\![RG]\!]$, and it acts on $B \widehat{\otimes}_R [\![RG]\!]$ diagonally).

Proof. This corresponds to the case $H = 1$ in Proposition 5.8.1. □

Proposition 5.8.3 *Let R be a profinite commutative ring, G a profinite group, and let $A, P \in$ **PMod**$([\![RG]\!])$. Assume that P is projective as an $[\![RG]\!]$-module and A is projective as an R-module. Then*

$$P \widehat{\otimes}_R A,$$

endowed with the diagonal G-action, is projective in **PMod**$([\![RG]\!])$.

Proof. Since P is a direct summand of a free $[\![RG]\!]$-module (see Proposition 5.4.2), we may assume that P is a free $[\![RG]\!]$-module. Hence (see Proposition 5.7.1) $P = [\![R(G \times Z)]\!]$, where Z is a profinite space, and G acts on $G \times Z$ by left multiplication on G. Note that A is a direct summand of some free profinite R-module $[\![RX]\!]$. Now, there exists a natural isomorphism of right $[\![RG]\!]$-modules

$$P \widehat{\otimes}_R [\![RX]\!] = [\![R(G \times Z)]\!] \widehat{\otimes}_R [\![RX]\!] \cong [\![R(G \times Z \times X)]\!],$$

where G acts on $P \widehat{\otimes}_R [\![RX]\!]$ via its left action on P, and on $[\![R(G \times Z \times X)]\!]$ via multiplication on the left of the component G of $G \times Z \times X$. Moreover, $P \widehat{\otimes}_R A$ with G-action induced from the action of G on P is obviously a direct summand of $P \widehat{\otimes}_R [\![RX]\!]$, and hence of $[\![R(G \times Z \times X)]\!]$. Therefore $P \widehat{\otimes}_R A$ with this action is a projective $[\![RG]\!]$-module by Corollary 5.7.2. Finally observe that $P \widehat{\otimes}_R A$ with this action is $[\![RG]\!]$-isomorphic to $P \widehat{\otimes}_R A$ with the diagonal action; indeed, $(g, z) \widehat{\otimes} a \mapsto (g, z) \widehat{\otimes} ga$ defines an $[\![RG]\!]$-isomorphism with inverse map given by $(g, z) \widehat{\otimes} a \mapsto (g, z) \widehat{\otimes} g^{-1}a$ ($a \in A, z \in Z, g \in G$). □

Dualizing the above three results one obtains the following.

Exercise 5.8.4 Let $H \leq_c G$ be profinite groups, R a commutative profinite ring, and let $A \in$ **DMod**$([\![RG]\!])$. Then

(a) There exists an isomorphism of $[\![RG]\!]$-modules

$$\mathrm{Hom}_{[\![RH]\!]}([\![RG]\!], A) \cong \mathrm{Hom}_R([\![R(G/H)]\!], A)$$

(the action of G on $\mathrm{Hom}_{[\![RH]\!]}([\![RG]\!], A)$ is given by $(xf)(g) = f(gx)$, and on $\mathrm{Hom}_R([\![R(G/H)]\!], A)$ it is diagonal, i.e., $(xf)(gH) = xf(xgH)$).

(b) Let A_0 denote the underlying R-module of A. Then there is an isomorphism of $[\![RG]\!]$-modules

$$\mathrm{Hom}_R([\![RG]\!], A_0) \cong \mathrm{Hom}_R([\![RG]\!], A)$$

given by $f \mapsto \bar{f}$, where $\bar{f}(g) = gf(g)$ ($f \in \mathrm{Hom}_R([\![RG]\!], A_0), \bar{f} \in \mathrm{Hom}_R([\![RG]\!], A), g \in G$; the actions are as indicated in part (a)).

(c) If A is injective as an R-module, and P is a projective $[\![RG]\!]$-module, then

$$\mathrm{Hom}_R(P, A),$$

with diagonal G-action, is injective in $\mathbf{DMod}([\![RG]\!])$.

5.9 Notes, Comments and Further Reading

There are accounts of discrete modules in Serre [1995], Ribes [1970] and Shatz [1972]. Profinite modules are special cases of pseudocompact modules over pseudocompact rings, defined in Brumer [1966].

The implication (b) ⇒ (c) of Proposition 5.1.2 appears in Goldman and Sah [1966].

Complete group algebras and complete tensor products are defined in Lazard [1965]. This monograph contains a general treatment of filtrations in pro-p groups and their relationship with mixed Lie algebras. It has a good account of analytic pro-p groups including cohomological results of Lazard which do not appear anywhere else.

5.9.1 The Magnus Algebra and Free Pro-p Groups

Let $M_p(n)$ denote the associative $\mathbf{Z}_p$-algebra of formal power series on the noncommuting indeterminates $u_1, \dots, u_n$ with coefficients in $\mathbf{Z}_p$. Endow $M_p(n)$ with the topology of simple convergence of the coefficients (in other words, the product topology of copies of $\mathbf{Z}_p$ indexed by the monomials on $u_1, \dots, u_n$). This is sometimes called a Magnus algebra. The results in the following theorem are due to M. Lazard.

Theorem 5.9.1 (Lazard [1965], Section II.3)

(a) *Let U be the multiplicative group of units of $M_p(n)$ consisting of those power series whose independent term is* 1. *Then U is a pro-p group.*

(b) *Let $F = F(x_1, \dots, x_n)$ be a free pro-p group of rank n on a basis $\{x_1, \dots, x_n\}$. Then the continuous homomorphism*

$$\varphi : F \longrightarrow U$$

determined by $\varphi(x_i) = 1 + u_i$ $(i = 1, \dots, n)$ is an embedding.

(c) *The map* φ *extends to a continuous isomorphism of* $\mathbf{Z}_p$*-algebras*

$$[\![\mathbf{Z}_p F]\!] \longrightarrow M_p(n).$$

It was pointed out by C.-K. Lim that these results can be extended to get

Corollary 5.9.2 (Lim [1973b]) *Let* $M(n)$ *be the associative* $\widehat{\mathbf{Z}}$*-algebra of formal power series on* n *noncommuting indeterminates with coefficients in* $\widehat{\mathbf{Z}}$*, and let* F_{nilp} *be the free pronilpotent group of rank* n*. Then statements analogous to* (a), (b), (c) *in the theorem above hold for* F_{nilp} *and* $M(n)$*.*

Lemma 5.6.5 appears as an exercise in Serre [1995] (only in the fifth edition of this book, page 4).

The nonexistence of continuous sections of the type presented in Example 5.6.8, has been known for a long time (cf. Ščepin [1976], pp. 157–158, from which such examples can be deduced). The version presented here as well a the content of Exercise 5.6.9 were communicated to us by C. Scheiderer. See Chatzidakis and Pappas [1992] for a more general version.

For the group of units in the ring of power series over a finite ring, see Deschamps and Leloup [2006].

6 Homology and Cohomology of Profinite Groups

6.1 Review of Homological Algebra

In this section we introduce some terminology and sketch some general homological results. For more details the reader may consult, e.g., Grothendieck [1957], Cartan and Eilenberg [1956] or Mac Lane [1963]. We shall state the concepts and results for general abelian categories to avoid repetitions, but we are mainly interested in categories of modules such as $\mathbf{Mod}(\Lambda)$, $\mathbf{PMod}(\Lambda)$ $\mathbf{DMod}(\Lambda)$ or $\mathbf{DMod}(G)$, where Λ is a profinite ring and G a profinite group. All functors will be assumed to be additive, i.e., they preserve direct sums systems of the form $A \oplus B$.

Let $\mathcal{B}$ and $\mathcal{D}$ be abelian categories. A *covariant cohomological functor*

$$\mathbf{H}^\bullet = \{H^n\}_{n\in\mathbf{Z}} : \mathcal{B} \longrightarrow \mathcal{D}$$

from $\mathcal{B}$ to $\mathcal{D}$ is a sequence of covariant additive functors $H^n : \mathcal{B} \longrightarrow \mathcal{D}$ that assigns to every short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

in $\mathcal{B}$ and every $n \in \mathbf{Z}$, a *connecting morphism*

$$\delta = \delta^n : H^n(C) \longrightarrow H^{n+1}(A)$$

satisfying the following conditions:

(a) For every commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\
0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0
\end{array}$$

in $\mathcal{B}$ with exact rows, the following diagram commutes for every n

$$\begin{array}{ccc}
H^n(C) & \xrightarrow{\delta^n} & H^{n+1}(A) \\
{\scriptstyle H^n(\gamma)}\downarrow & & \downarrow{\scriptstyle H^{n+1}(\alpha)} \\
H^n(C') & \xrightarrow{\delta^n} & H^{n+1}(A')
\end{array}$$

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4_6,

(b) The long sequence

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

is exact.

Analogously, a *contravariant cohomological functor* $\mathbf{H}^\bullet = \{H^n\}_{n\in\mathbf{Z}} : \mathcal{B} \longrightarrow \mathcal{D}$ from $\mathcal{B}$ to $\mathcal{D}$ is a sequence of contravariant additive functors $H^n : \mathcal{B} \longrightarrow \mathcal{D}$, with connecting morphisms $\delta^n : H^n(A) \longrightarrow H^{n+1}(C)$, and satisfying conditions similar to (a) and (b). A *covariant homological functor* $\mathbf{H}_\bullet = \{H_n\}_{n\in\mathbf{Z}}$ from $\mathcal{B}$ to $\mathcal{D}$ is a sequence of covariant additive functors $H_n : \mathcal{B} \longrightarrow \mathcal{D}$, with connecting morphisms $\delta_n : H_n(C) \longrightarrow H_{n-1}(A)$ and satisfying conditions similar to (a) and (b). Finally, a *contravariant homological functor* $\mathbf{H}_\bullet = \{H_n\}_{n\in\mathbf{Z}} : \mathcal{B} \longrightarrow \mathcal{D}$ from $\mathcal{B}$ to $\mathcal{D}$ is a sequence of contravariant additive functors $H_n : \mathcal{B} \longrightarrow \mathcal{D}$, with connecting morphisms $\delta_n : H_n(A) \longrightarrow H_{n-1}(C)$ and satisfying conditions similar to (a) and (b).

Let $\mathcal{B}^{op} \longrightarrow \mathcal{B}$, $\mathcal{B} \longrightarrow \mathcal{B}^{op}$ and $\mathcal{D} \longrightarrow \mathcal{D}^{op}$ be the canonical contravariant functors from a category to its opposite category. Then the following statements are equivalent:

(a) $\mathbf{H}^\bullet : \mathcal{B} \longrightarrow \mathcal{D}$ is a covariant cohomological functor;

(b) $\mathcal{B}^{op} \longrightarrow \mathcal{B} \xrightarrow{\mathbf{H}^\bullet} \mathcal{D}$ is a contravariant cohomological functor;

(c) $\mathcal{B} \xrightarrow{\mathbf{H}^\bullet} \mathcal{D} \longrightarrow \mathcal{D}^{op}$ is a contravariant homological functor;

(d) $\mathcal{B}^{op} \longrightarrow \mathcal{B} \xrightarrow{\mathbf{H}^\bullet} \mathcal{D} \longrightarrow \mathcal{D}^{op}$ is a covariant homological functor.

Therefore, a statement made about one of these (co)homological functors has an automatic translation to a corresponding statement about any of the other three (co)homological functors. Hence it suffices to consider one of these types of (co)homological functors; we shall usually state definitions and results for covariant cohomological functors.

Let $\mathbf{H}^\bullet, \mathbf{T}^\bullet$ be covariant cohomological functors from $\mathcal{B}$ to $\mathcal{D}$. A *morphism* $\varphi : \mathbf{H}^\bullet \longrightarrow \mathbf{T}^\bullet$ is a family $\varphi^n : H^n \longrightarrow T^n$ $(n \in \mathbf{Z})$ of morphisms of functors such that for every short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

in $\mathcal{B}$, the following diagram commutes:

$$\begin{array}{ccc} H^n(C) & \xrightarrow{\delta^n} & H^{n+1}(A) \\ {\scriptstyle \varphi^n(C)}\downarrow & & \downarrow{\scriptstyle \varphi^{n+1}(A)} \\ T^n(C) & \xrightarrow{\delta^n} & T^{n+1}(A) \end{array}$$

for every $n \in \mathbf{Z}$.

An additive functor $F : \mathcal{B} \longrightarrow \mathcal{D}$ is called *effaceable* if for every object A of $\mathcal{B}$ there is a monomorphism $\iota : A \longrightarrow B$ such that $F(\iota) = 0$. Dually F is called *coeffaceable* if for every object A of $\mathcal{B}$ there is an epimorphism $\pi : B \longrightarrow A$ such that $F(\pi) = 0$.

We say that F is *effaceable by* a class of objects $\mathcal{M}$ of C if $F(M) = 0$ for every $M \in \mathcal{M}$.

Recall that a category $\mathcal{B}$ has enough projectives (respectively, enough injectives) if for each object A in $\mathcal{B}$, there exists an epimorphism $P \longrightarrow A$ in $\mathcal{B}$, where P is projective (respectively, a monomorphism $A \longrightarrow Q$ in $\mathcal{B}$, where Q is injective).

Lemma 6.1.1 *Let $F : \mathcal{B} \longrightarrow \mathcal{D}$ be an additive functor of abelian categories.*

(a) *If F is effaceable, then $F(Q) = 0$ for every injective object Q of $\mathcal{B}$.*
(a′) *If F is coeffaceable, then $F(P) = 0$ for every projective object P of $\mathcal{B}$.*
(b) *Assume that $\mathcal{B}$ has enough injectives. Then, F is effaceable if and only if $F(Q) = 0$ for every injective object Q of $\mathcal{B}$.*
(b′) *Assume that $\mathcal{B}$ has enough projectives. Then, F is coeffaceable if and only if $F(P) = 0$ for every projective object P of $\mathcal{B}$.*

Proof. Let Q be injective, and suppose that $\varphi : Q \longrightarrow M$ is a monomorphism such that $F(\varphi) = 0$. By definition of injective object, there exists a morphism $\psi : M \longrightarrow Q$ with $\psi\varphi = \mathrm{id}_Q$. Hence $F(\mathrm{id}_Q) = 0$, and so $F(Q) = 0$. This proves (a). Part (b) follows immediately from (a). Statements (a′) and (b′) are obtained from (a) and (b) by duality. □

Let $\mathbf{H}^\bullet$ be a *positive covariant cohomological functor*, from $\mathcal{B}$ to $\mathcal{D}$, i.e., a covariant cohomological functor such that $H^n = 0$ for $n < 0$. We say that $\mathbf{H}^\bullet$ is *effaceable* if H^n is effaceable for every $n > 0$. There are similar definitions for *positive coeffaceable contravariant cohomological functor* and *positive coeffaceable covariant homological functor*.

Before stating the following proposition we need some more terminology. We say that a positive cohomological functor $\mathbf{H}^\bullet : \mathcal{B} \longrightarrow \mathcal{D}$ is *universal* if it satisfies the following condition: whenever $\mathbf{E}^\bullet : \mathcal{B} \longrightarrow \mathcal{D}$ is a cohomological functor of the same type, then for every morphism of functors $\psi : H^0 \longrightarrow E^0$ there exists a unique morphism $\varphi : \mathbf{H}^\bullet \longrightarrow \mathbf{E}^\bullet$ with $\varphi^0 = \psi$. Dually, a positive homological functor $\mathbf{H}_\bullet : \mathcal{B} \longrightarrow \mathcal{D}$ is *universal* if whenever $\mathbf{E}_\bullet : \mathcal{B} \longrightarrow \mathcal{D}$ is a homological functor of the same type, then for every morphism of functors $\psi : E_0 \longrightarrow H_0$ there exists a unique morphism $\varphi : \mathbf{E}_\bullet \longrightarrow \mathbf{H}_\bullet$ with $\varphi_0 = \psi$.

Proposition 6.1.2 *Let $\mathbf{H}^\bullet$ be a positive cohomological functor from $\mathcal{B}$ to $\mathcal{D}$. Assume that $\mathcal{B}$ has enough injectives and that $\mathbf{H}^\bullet$ is effaceable. Then $\mathbf{H}^\bullet$ is universal.*

Proof. To fix the ideas, we shall assume that $\mathbf{H}^\bullet$ is covariant; the contravariant case is similar. We just sketch the proof and leave the details to the reader.

Consider a cohomological functor $\mathbf{E}^\bullet : \mathcal{B} \longrightarrow \mathcal{D}$ of the same type, and let $\psi : H^0 \longrightarrow E^0$ be a morphism of functors. For $A \in \mathcal{B}$, let

$$0 \longrightarrow A \longrightarrow M_A \longrightarrow X_A \longrightarrow 0$$

be exact in $\mathcal{B}$, with M_A injective.

To prove the existence of φ we proceed by induction. Suppose the existence of morphisms $\varphi^i : H^i \longrightarrow E^i$, $i = 0, 1, \ldots, n-1$, has already been shown, with $\varphi^0 = \psi$, and that they commute with the connecting homomorphisms δ. Define $\varphi^n(A) : H^n(A) \longrightarrow E^n(A)$ to be the unique map making the following diagram commutative

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & H^{n-1}(M_A) & \longrightarrow & H^{n-1}(X_A) & \xrightarrow{\delta} & H^n(A) & \longrightarrow & 0 \\
& \downarrow & & \downarrow{\scriptstyle \varphi^{n-1}(X_A)} & & \downarrow{\scriptstyle \varphi^n(A)} & & \downarrow \\
\cdots \longrightarrow & E^{n-1}(M_A) & \longrightarrow & E^{n-1}(X_A) & \xrightarrow{\delta} & E^n(A) & \longrightarrow & E^n(M_A)
\end{array}$$

Now, it is straightforward to check that φ^n is a morphism of functors, and that $\varphi^0, \varphi^1, \ldots, \varphi^n$ commute with the connecting homomorphisms δ.

For the uniqueness of φ, suppose $\bar{\varphi} : \mathbf{H}^\bullet \longrightarrow \mathbf{E}^\bullet$ is another morphism with $\bar{\varphi}^0 = \psi$. Assume $\varphi^{n-1} = \bar{\varphi}^{n-1}$. Then from the commutativity of

$$\begin{array}{ccccccc}
\cdots \longrightarrow & H^{n-1}(X_A) & \longrightarrow & H^n(A) & \longrightarrow & 0 & \longrightarrow \cdots \\
& \downarrow & & {\scriptstyle \varphi^n(A)}\downarrow{\scriptstyle \bar{\varphi}^n(A)} & & \downarrow & \\
\cdots \longrightarrow & E^{n-1}(X_A) & \longrightarrow & E^n(A) & \longrightarrow & E^n(M_A) & \longrightarrow \cdots
\end{array}$$

it follows that $\varphi^n(A) = \bar{\varphi}^n(A)$, for all $A \in \mathcal{B}$; hence $\varphi^n = \bar{\varphi}^n$; thus $\varphi = \bar{\varphi}$ by induction. $\square$

Dually, one obtains

Proposition 6.1.3 *Let $\mathbf{H}_\bullet$ be a positive homological functor from $\mathcal{B}$ to $\mathcal{D}$. Assume that $\mathcal{B}$ has enough projectives and that $\mathbf{H}_\bullet$ is coeffaceable. Then $\mathbf{H}_\bullet$ is universal.*

The following result follows from the definition of universality. It is often used in conjunction with Propositions 6.1.2 and 6.1.3.

Lemma 6.1.4

(a) *Let $\mathbf{H}^\bullet$, $\mathbf{F}^\bullet$ be universal cohomological functors from $\mathcal{B}$ to $\mathcal{D}$ of the same type. Let*

$$H^0 \overset{\psi}{\to} F^0$$

be a morphism of functors, and

$$\mathbf{H}^\bullet \overset{\varphi}{\to} \mathbf{F}^\bullet$$

its corresponding extension. Then φ is an isomorphism if and only if ψ is an isomorphism.

(b) *Dually, let $\mathbf{H}_\bullet$, $\mathbf{F}_\bullet$ be universal homological functors from $\mathcal{B}$ to $\mathcal{D}$ of the same type. Let*

$$H_0 \overset{\psi}{\to} F_0$$

be a morphism of functors, and

$$\mathbf{H}_\bullet \overset{\varphi}{\to} \mathbf{F}_\bullet$$

its corresponding extension. Then φ is an isomorphism if and only if ψ is an isomorphism.

Right and Left Derived Functors

A covariant (respectively, contravariant) functor $F : \mathcal{B} \longrightarrow \mathcal{D}$ from an abelian category $\mathcal{B}$ to an abelian category $\mathcal{D}$ is called *left exact* if whenever

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is a short exact sequence in $\mathcal{B}$, then

$$0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C)$$

is exact (respectively,

$$0 \longrightarrow F(C) \longrightarrow F(B) \longrightarrow F(A)$$

is exact). There is an analogous definition for *right exact* functors. Let $F : \mathcal{B} \longrightarrow \mathcal{D}$ be a left exact covariant functor, and assume that $\mathcal{B}$ has enough injectives. Then, associated with F there is a (unique) positive effaceable universal covariant cohomological functor $\{R^nF\}_{n\geq 0}$ from $\mathcal{B}$ to $\mathcal{D}$, with $R^0F = F$ called the sequence of *right derived functors* of F. This sequence is constructed as follows. Given an object A in $\mathcal{B}$, let

$$0 \longrightarrow A \longrightarrow Q^0 \longrightarrow \cdots \longrightarrow Q^n \overset{d^n}{\longrightarrow} Q^{n+1} \longrightarrow \cdots$$

be an *injective resolution* of A (i.e., an exact sequence where each Q^n is injective in $\mathcal{B}$). Define $R^nF(A)$ to be the *n-th cohomology group* of the cochain complex

$$0 \longrightarrow F(Q^0) \longrightarrow \cdots \longrightarrow F(Q^n) \overset{F(d^n)}{\longrightarrow} F(Q^{n+1}) \longrightarrow \cdots$$

i.e, $R^nF(A) = \mathrm{Ker}(F(d^n))/\mathrm{Im}(F(d^{n-1}))$.

Since F is left exact, $F(A) = R^0F(A)$. It is not difficult, but it requires some patience, to check that in fact this defines a universal covariant cohomological functor. The reader may consult, e.g., Cartan and Eilenberg [1956], Mac Lane [1963] or Grothendieck [1957] for the details.

Similarly, if $F : \mathcal{B} \longrightarrow \mathcal{D}$ is a left exact contravariant functor and $\mathcal{B}$ has enough projectives, then, associated with F there is a (unique) positive coeffaceable universal contravariant cohomological functor $\{R^nF\}_{n\geq 0}$ from $\mathcal{B}$ to $\mathcal{D}$, with $R^0F = F$, called the sequence of *right derived functors* of F. This sequence is constructed as follows.

Given an object A in $\mathcal{B}$, let

$$\cdots \longrightarrow P_{n+1} \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

be a *projective resolution* of A (i.e., an exact sequence where each P_n is projective in $\mathcal{B}$). Define $R^nF(A)$ to be the n-th cohomology group of the cochain complex

$$0 \longrightarrow F(P_0) \longrightarrow \cdots \longrightarrow F(P_n) \longrightarrow F(P_{n+1}) \longrightarrow \cdots.$$

If $F : \mathcal{B} \longrightarrow \mathcal{D}$ is a right exact covariant functor and $\mathcal{B}$ has enough projectives, then, associated with F there is a (unique) positive coeffaceable universal covariant homological functor $\{L_nF\}_{n\geq 0}$ from $\mathcal{B}$ to $\mathcal{D}$, with $L_0F = F$ called the sequence of *left derived functors* of F. This sequence is constructed as follows.

Given an object A in $\mathcal{B}$, let

$$\cdots \longrightarrow P_{n+1} \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

be a projective resolution of A. Define $L^nF(A)$ to be the n-th homology group of the chain complex

$$\cdots \longrightarrow F(P_{n-1}) \longrightarrow F(P_n) \longrightarrow \cdots \longrightarrow F(P_0) \longrightarrow 0.$$

Bifunctors

Let $\mathcal{B}$, $\mathcal{B}'$ and $\mathcal{D}$ be abelian categories. A functor of the type

$$F = F(-,-) : \mathcal{B} \times \mathcal{B}' \longrightarrow \mathcal{D}$$

is sometimes called a *bifunctor* from $\mathcal{B} \times \mathcal{B}'$ to $\mathcal{D}$. Fix an object $A \in \mathcal{B}$, then

$$F(A,-) : \mathcal{B}' \longrightarrow \mathcal{D}$$

is a functor. Similarly if $A' \in \mathcal{B}'$, then

$$F(-,A') : \mathcal{B} \longrightarrow \mathcal{D}$$

is a functor. We refer to $F(A,-)$ as the functor on the second variable (attached to A), and to $F(-,A')$ as the functor on the first variable (attached to A'). Then one may calculate the derived functors of these two functors. The following two results indicate that under certain conditions these derived functors coincide. For the proofs one may consult Grothendieck [1957], page 144, and in slightly less generality Cartan and Eilenberg [1956], pages 94–97.

Theorem 6.1.5 *Let $F = F(-,-) : \mathcal{B} \times \mathcal{B}' \longrightarrow \mathcal{D}$ be a bifunctor. Assume*

(a) *$F(-,-)$ is covariant and left exact on the second variable and contravariant and left exact on the first one.*
(b) *$F(P,-)$ is exact whenever P is a projective object of $\mathcal{B}$ and $F(-,Q)$ is exact whenever Q is an injective object of $\mathcal{B}'$.*
(c) *$\mathcal{B}$ has enough projectives and $\mathcal{B}'$ has enough injectives.*

Fix objects $A \in \mathcal{B}$ and $B \in \mathcal{B}'$, and denote the functor $F(-,B)$ by F_1 and the functor $F(A,-)$ by F_2. Then

$$(R^n F_1)(A) = (R^n F_2)(B) \quad \text{for all } n \geq 0.$$

Theorem 6.1.6 *Let $F = F(-,-) : \mathcal{B} \times \mathcal{B}' \longrightarrow \mathcal{D}$ be a bifunctor. Assume*

(a) *$F(-,-)$ is covariant and right exact on the first and second variables.*
(b) *$F(P,-)$ and $F(-,P')$ are exact whenever P is a projective object of $\mathcal{B}$ and P' a projective object of $\mathcal{B}'$, respectively.*
(c) *$\mathcal{B}$ and $\mathcal{B}'$ have enough projectives.*

Fix the objects $A \in \mathcal{B}$ and $B \in \mathcal{B}'$, and denote the functor $F(-,B)$ by F_1 and $F(A,-)$ by F_2. Then

$$(L_n F_1)(A) = (L_n F_2)(B), \quad \text{for all } n \geq 0.$$

The Ext Functors

Next we apply these general results to the concrete categories of modules over profinite rings and groups that are of interest to us.

Let Λ be a profinite R-algebra, where R is a commutative profinite ring (see Section 5.1). Consider now the bifunctor $\operatorname{Hom}_\Lambda(-,-)$ from the category $\mathbf{PMod}(\Lambda) \times \mathbf{DMod}(\Lambda)$ to the category $\mathbf{DMod}(R)$; it is covariant on the second variable and contravariant on the first one. Fix $A \in \mathbf{PMod}(\Lambda)$. Denote by $\operatorname{Ext}^n_\Lambda(A,-)$ the n-th right derived functor of the functor

$$\operatorname{Hom}_\Lambda(A,-) : \mathbf{DMod}(\Lambda) \longrightarrow \mathbf{DMod}(R).$$

Note that $\operatorname{Hom}_\Lambda(-,-)$ satisfies the hypotheses of Theorem 6.1.5 (see Exercise 5.4.7). Hence if $B \in \mathbf{DMod}(\Lambda)$, then $\operatorname{Ext}^n_\Lambda(A,B)$ can also be computed by obtaining the n-th right derived functor of

$$\mathrm{Hom}_\Lambda(-,B) : \mathbf{PMod}(\Lambda) \longrightarrow \mathbf{DMod}(R)$$

and then applying it to A.

Putting together the above information, we get the following characterization of the functor $\mathrm{Ext}^n_\Lambda(-,-)$.

Proposition 6.1.7 *Let R be a commutative profinite ring and Λ a profinite R-algebra. Fix $A \in \mathbf{PMod}(\Lambda)$ and $B \in \mathbf{DMod}(\Lambda)$. Then*

(a) $\{\mathrm{Ext}^n_\Lambda(A,-)\}_{n\in\mathbf{N}}$ *is the unique positive covariant cohomological functor from $\mathbf{DMod}(\Lambda)$ to $\mathbf{DMod}(R)$ such that $\mathrm{Ext}^n_\Lambda(A,Q) = 0$ for $n \geq 1$ and for every injective discrete Λ-module Q. Moreover,* $\mathrm{Ext}^0_\Lambda(A,-) = \mathrm{Hom}_\Lambda(A,-)$.

(b) $\{\mathrm{Ext}^n_\Lambda(-,B)\}_{n\in\mathbf{N}}$ *is the unique positive contravariant cohomological functor from $\mathbf{PMod}(\Lambda)$ to $\mathbf{DMod}(R)$ such that $\mathrm{Ext}^n_\Lambda(P,B) = 0$ for $n \geq 1$ and for every projective profinite Λ-module P. Moreover,* $\mathrm{Ext}^0_\Lambda(-,B) = \mathrm{Hom}_\Lambda(-,B)$.

In particular $\mathrm{Ext}^n_\Lambda(A,-)$ and $\mathrm{Ext}^n_\Lambda(-,B)$ are additive functors, i.e., they commute with finite direct sums.

As a consequence of this proposition together with Lemmas 5.1.4 and 6.1.4, we get that each of the functors $\mathrm{Ext}^n_\Lambda(A,-)$ and $\mathrm{Ext}^n_\Lambda(-,B)$ commutes with limits ($n \geq 0$). Explicitly,

Corollary 6.1.8 *Under the hypotheses of the above proposition, we have*

(a)

$$\mathrm{Ext}^n_\Lambda\Big(A, \varinjlim_{i\in I} B_i\Big) = \varinjlim_{i\in I} \mathrm{Ext}^n_\Lambda(A,B_i),$$

where $\{B_i, \psi_{ij}, I\}$ is a direct system of discrete Λ-modules.

(b)

$$\mathrm{Ext}^n_\Lambda\Big(\varprojlim_{i\in I} A_i, B\Big) = \varinjlim_{i\in I} \mathrm{Ext^n}_\Lambda(A_i,B),$$

where $\{A_i, \varphi_{ij}, I\}$ is a surjective inverse system of profinite Λ-modules.

The Tor Functors

Next we consider the bifunctor

$$-\,\widehat{\otimes}_\Lambda\,- : \mathbf{PMod}(\Lambda^{op}) \times \mathbf{PMod}(\Lambda) \longrightarrow \mathbf{PMod}(R).$$

Let A be a profinite right Λ-module. Then

$$A\,\widehat{\otimes}_\Lambda\,- : \mathbf{PMod}(\Lambda) \longrightarrow \mathbf{PMod}(R)$$

is a right exact covariant functor. Since $\mathbf{PMod}(\Lambda)$ has enough projectives (see Proposition 5.4.2), there exist left derived functors of $A\,\widehat{\otimes}_\Lambda\,-$. We define the n-th *Tor functor* $\mathrm{Tor}_n^{\Lambda}(A,-)$ as the n-th derived functor of $A \widehat{\otimes}_{\Lambda} -$. Let B be a left Λ-module. According to Theorem 6.1.6, $\mathrm{Tor}_n^{\Lambda}(A,B)$ can also be computed by taking the n-th left derived functor of $- \widehat{\otimes}_{\Lambda} B$ and applying it to A.

Using this notation, we get the following characterization of the functors $\mathrm{Tor}_n^{\Lambda}(-,-)$.

Proposition 6.1.9 *Let R be a commutative profinite ring and Λ a profinite R-algebra. Fix $A \in \mathbf{PMod}(\Lambda^{op})$ and $B \in \mathbf{PMod}(\Lambda)$. Then*

(a) $\{\mathrm{Tor}_n^{\Lambda}(A,-)\}_{n\in\mathbf{N}}$ *is the unique positive covariant homological functor from $\mathbf{PMod}(\Lambda)$ to $\mathbf{PMod}(R)$ such that $\mathrm{Tor}_n^{\Lambda}(A,P) = 0$, for $n \geq 1$ and for every projective profinite Λ-module P. Moreover,* $\mathrm{Tor}_0^{\Lambda}(A,-) = A \widehat{\otimes}_{\Lambda} -$.

(b) $\{\mathrm{Tor}_n^{\Lambda}(-,B)\}_{n\in\mathbf{N}}$ *is the unique positive covariant homological functor from $\mathbf{PMod}(\Lambda^{op})$ to $\mathbf{PMod}(R)$ such that $\mathrm{Tor}_n^{\Lambda}(P,B) = 0$, for $n \geq 1$ and for every projective profinite right Λ-module P. Moreover,* $\mathrm{Tor}_0^{\Lambda}(-,B) = - \widehat{\otimes}_{\Lambda} B$.

In particular $\mathrm{Tor}_n^{\Lambda}(A,-)$ and $\mathrm{Tor}_n^{\Lambda}(-,B)$ are additive functors, i.e., they commute with finite direct sums.

It follows from this proposition, Lemma 5.5.2 and Lemma 6.1.4 that each of the functors $\mathrm{Tor}_n^{\Lambda}(A,-)$ and $\mathrm{Tor}_n^{\Lambda}(-,B)$ commutes with inverse limits ($n \geq 0$). Explicitly,

Corollary 6.1.10 *Under the hypotheses of the above proposition, we have*

(a)
$$\mathrm{Tor}_n^{\Lambda}(A, \varprojlim_{i\in I} B_i) = \varprojlim_{i\in I} \mathrm{Tor}_n^{\Lambda}(A, B_i),$$
where $\{B_i, \psi_{ij}, I\}$ is an inverse system of profinite Λ-modules.

(b)
$$\mathrm{Tor}_n^{\Lambda}(\varprojlim_{i\in I} A_i, B) = \varprojlim_{i\in I} \mathrm{Tor}_n^{\Lambda}(A_i, B),$$
where $\{A_i, \varphi_{ij}, I\}$ is an inverse system of profinite right Λ-modules.

6.2 Cohomology with Coefficients in $\mathbf{DMod}(⟦RG⟧)$

Let G be a profinite group and R a commutative profinite ring. Consider R as a profinite G-module with trivial action: $gr = r$ for all $g \in G$, $r \in R$. Then R becomes an $⟦RG⟧$-module. Given a discrete $⟦RG⟧$-module A define the *n-th cohomology group* $H^n(G,A)$ of G with coefficients in A by

$$H^n(G,A) = \mathrm{Ext}^n_{⟦RG⟧}(R,A) \quad (n \in \mathbf{N}).$$

It follows that

$$H^0(G,A) = \mathrm{Ext}^0_{[\![RG]\!]}(R,A) = \mathrm{Hom}_{[\![RG]\!]}(R,A).$$

On the other hand, every homomorphism φ in $\mathrm{Hom}_{[\![RG]\!]}(R,A)$ is completely determined by its value on the element 1 of R; therefore, φ can be identified with an element a of A which is fixed by the action of G, i.e., $ga = a$ for every $g \in G$. Recall (see Lemma 5.3.1) that the subgroup of fixed points of A under the action of G is defined by

$$A^G = \{a \mid a \in A, ga = a, \forall g \in G\}.$$

It is evident that A^G is an $[\![RG]\!]$-submodule of A. We call A^G the *submodule of fixed points* of A. Hence we have

Lemma 6.2.1 *Let G be a profinite group. There is an isomorphism of R-modules*

$$H^0(G,A) = \mathrm{Hom}_{[\![RG]\!]}(R,A) \cong A^G$$

for every $A \in \mathbf{DMod}([\![RG]\!])$, and this isomorphism is functorial on the variable A.

Sometimes we use the notation $(-)^G$ for the functor that assigns to each $[\![RG]\!]$-module A, the submodule A^G of fixed points.

The following characterization is a consequence of Proposition 6.1.7 and Lemma 6.2.1.

Proposition 6.2.2 *Let G be a profinite group. Then,*

$$\{H^n(G,-)\}_{n\in\mathbf{N}}$$

is the sequence of right derived functors of the functor $A \mapsto A^G$ from $\mathbf{DMod}([\![RG]\!])$ to $\mathbf{DMod}(R)$. In other words, $\mathbf{H}^\bullet(G,-) = \{H^n(G,-)\}_{n\in\mathbf{N}}$ is the unique sequence of functors from $\mathbf{DMod}([\![RG]\!])$ to $\mathbf{DMod}(R)$ such that

(a) $H^0(G,A) = A^G$ *(as functors on $\mathbf{DMod}([\![RG]\!])$);*
(b) $H^n(G,Q) = 0$ *for every discrete injective $[\![RG]\!]$-module Q and $n \geq 1$;*
(c) *For each short exact sequence $0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0$ in $\mathbf{DMod}([\![RG]\!])$, there exist connecting homomorphisms*

$$\delta : H^n(G,A_3) \longrightarrow H^{n+1}(G,A_1)$$

for all $n \geq 0$, such that the sequence

$$\begin{aligned} 0 \to H^0(G,A_1) \to H^0(G,A_2) \to H^0(G,A_3) \\ \xrightarrow{\delta} H^1(G,A_1) \to H^1(G,A_2) \to \cdots \end{aligned}$$

is exact; and

(d) *For every commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A_1' & \longrightarrow & A_2' & \longrightarrow & A_3' & \longrightarrow & 0 \end{array}$$

in **DMod**($[\![RG]\!]$) *with exact rows, the following diagram commutes for every* $n \geq 0$

$$\begin{array}{ccc} H^n(G, A_3) & \xrightarrow{\delta} & H^{n+1}(G, A_1) \\ {\scriptstyle H^n(G,\gamma)}\downarrow & & \downarrow{\scriptstyle H^{n+1}(G,\alpha)} \\ H^n(G, A_3') & \xrightarrow{\delta} & H^{n+1}(G, A_1') \end{array}$$

.

Standard Resolutions

Next we shall describe an explicit way of calculating the cohomology groups $H^n(G, A) = \mathrm{Ext}^n_{[\![RG]\!]}(R, A)$. First we construct convenient projective resolutions for the profinite $[\![RG]\!]$-module R. This can be done as in the case of abstract groups and modules.

The Homogeneous Bar Resolution

For each $n \geq 0$, define L_n as the left free profinite R-module on the free profinite G-space $G^{n+1} = G\times \overset{n+1}{\cdots} \times G$ with diagonal action (i.e., $x(x_1, \ldots, x_n) = (xx_1, \ldots, xx_n)$, for $x, x_1, \ldots, x_n \in G$). Then (see Proposition 5.7.1) L_n is a free profinite $[\![RG]\!]$-module on the profinite space

$$\{(1, x_1, \ldots, x_n) \mid x_i \in G\}.$$

Define a sequence $\mathbf{L}(G)$:

$$\cdots \longrightarrow L_n \xrightarrow{\partial_n} L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \xrightarrow{\epsilon} R \longrightarrow 0, \tag{1}$$

where

$$\partial_n(x_0, x_1, \ldots, x_n) = \sum_{i=0}^{n} (-1)^i (x_0, \ldots, \hat{x}_i, \ldots, x_n)$$

(the symbol $\hat{x}_i$ indicates that x_i is to be omitted), and ϵ is the augmentation map

$$\epsilon(x) = 1.$$

It is easy to check that ϵ and each ∂_n are $[\![RG]\!]$-homomorphisms, and that (1) is a chain complex (i.e., $\partial_n\partial_{n+1} = 0$ ($n \geq 1$) and $\varepsilon\partial_1 = 0$). In fact it is exact, and hence a free $[\![RG]\!]$-resolution of R. One way of verifying this is to establish the existence of a 'contracting homotopy', i.e., continuous R-homomorphisms $\gamma_n : L_n \longrightarrow L_{n+1}$ ($n \geq 0$) and $\gamma_{-1} : R \longrightarrow L_0$ such that $\partial_{n+1}\gamma_n + \gamma_{n-1}\partial_n =$ id, $\partial_1\gamma_0 + \gamma_{-1}\epsilon =$ id and $\epsilon\gamma_{-1} =$ id. Assume such contracting maps γ_n have been found; then the exactness of (1) follows immediately. Indeed, if $a \in L_n$ and $\partial_n(a) = 0$ (or $\epsilon(a) = 0$, if $n = 0$) put $b = \gamma_n(a)$; then $a = \partial_{n+1}(b)$, proving the assertion. We defined the maps γ_n as follows:

$$\gamma_n(x_0, x_1, \ldots, x_n) = (1, x_0, x_1, \ldots, x_n) \quad \text{and} \quad \gamma_{-1}(1) = (1).$$

It is easy to verify that these maps form indeed a contracting homotopy. The free resolution (1) of R is called the *homogeneous bar resolution*.

The Inhomogeneous Bar Resolution

It is sometimes convenient to work with a different free resolution of R. For each natural number $n = 0, 1, 2, \ldots$, let $\tilde{L}_n = \tilde{L}_n(G)$ be the free profinite left $[\![RG]\!]$-module on the topological basis $G^n = G \times \overset{n}{\cdots} \times G$ (notice that $\tilde{L}_0$ is just the free $[\![RG]\!]$-module on the space consisting of the single symbol (), i.e., $\tilde{L}_0 \cong [\![RG]\!]$, as modules). In this case, define the *augmentation map* $\tilde{\varepsilon} : L_0 \longrightarrow R$ as the continuous $[\![RG]\!]$-epimorphism such that $\tilde{\varepsilon}() = 1$. If $n \geq 1$, define $\tilde{\partial}_n : \tilde{L}_n \longrightarrow \tilde{L}_{n-1}$ to be the unique $[\![RG]\!]$-homomorphism extending the map $G^n \longrightarrow \tilde{L}_{n-1}$ given by

$$\tilde{\partial}_n(x_1, \ldots, x_n) = x_1(x_2, \ldots, x_n) + \sum_{i=1}^{n-1}(-1)^i(x_1, \ldots, x_i x_{i+1}, \ldots, x_n) + (-1)^n(x_1, \ldots, x_{n-1}).$$

Consider now the sequence $\tilde{\mathbf{L}}(G)$:

$$\cdots \longrightarrow \tilde{L}_n \xrightarrow{\tilde{\partial}_n} \tilde{L}_{n-1} \longrightarrow \cdots \longrightarrow \tilde{L}_0 \xrightarrow{\tilde{\varepsilon}} R \longrightarrow 0. \tag{2}$$

One checks without difficulty that (2) is a complex. To show that it is exact, one can define a contracting homotopy (see Exercise 6.2.3 below), but instead, we proceed by proving that (1) and (2) are isomorphic complexes. Let $\varphi_n : \tilde{L}_n \longrightarrow L_n$ and $\psi_n : L_n \longrightarrow \tilde{L}_n$ be given by

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

and by

$$\psi_n(x_0, x_1, \ldots, x_n) = x_0(x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_{n-1}^{-1}x_n).$$

Then φ_n and ψ_n are $[\![RG]\!]$-homorphisms, inverse to each other. Moreover $\partial_{n+1}\varphi_{n+1} = \varphi_n\tilde{\partial}_{n+1}$ ($n \geq 1$) and $\epsilon\varphi_0 = \tilde{\epsilon}$ (in other words, $\{\varphi_n\}_{n\geq 0}$ is an homomorphism of chain complexes); similarly, $\{\psi_n\}_{n\geq 0}$ is a homomorphism of chain complexes. Hence (1) and (2) are isomorphic complexes, and so (2) is exact. Thus (2) is a free (and thus projective) resolution of R. We call (2) the *inhomogeneous bar resolution* of R.

Exercise 6.2.3 Give a direct proof that (2) is an exact sequence by constructing a contracting homotopy.

Let $A \in \mathbf{DMod}([\![\mathbf{RG}]\!])$. Observe that if $f \in \mathrm{Hom}_{[\![RG]\!]}(L_n, A)$, then the image of f is finite since A is discrete and L_n compact; therefore, it follows from the freeness of L^n that

$$\mathrm{Hom}_{[\![RG]\!]}(L_n, A) \cong C^n(G, A),$$

where $C^n(G, A)$ consists of all continuous maps $f : G^{n+1} \longrightarrow A$ such that $f(xx_0, xx_1, \ldots, xx_n) = xf(x_0, x_1, \ldots, x_n)$, for all $x, x_i \in G$. Note that $C^n(G, A)$ is a discrete R-module, with module structure given by

$$(rf)(x_0, x_1, \ldots, x_n) = rf(x_0, x_1, \ldots, x_n) \quad r \in R, x, x_0, x_1, \ldots, x_n \in G.$$

The elements of $C^n(G, A)$ are called *homogeneous n-cochains.*

If one applies the functor $\mathrm{Hom}_{[\![RG]\!]}(-, A) = -^G$ to (2), excluding the first term R, one gets the following cochain complex, $\mathbf{C}(G, A)$:

$$0 \longrightarrow C^0(G, A) \longrightarrow \cdots \longrightarrow C^n(G, A) \stackrel{\partial^{n+1}}{\longrightarrow} C^{n+1}(G, A) \longrightarrow \cdots, \tag{3}$$

where

$$(\partial^{n+1} f)(x_0, x_1, \ldots, x_{n+1}) = \sum_{i=0}^{n+1} (-1)^i f(x_0, \ldots, \hat{x}_i, \ldots x_{n+1}). \tag{4}$$

Thus, according to the definition of cohomology groups of G with coefficients in $A \in \mathbf{DMod}([\![\mathbf{RG}]\!])$, we have the following explicit description:

Theorem 6.2.4 *$H^n(G, A)$ is the n-th cohomology group of the cochain complex (3), i.e.,*

$$H^n(G, A) = \mathrm{Ext}^n_{[\![RG]\!]}(R, A) = \mathrm{Ker}(\partial^{n+1})/\mathrm{Im}(\partial^n).$$

Following standard terminology, we refer to the elements in $\mathrm{Ker}(\partial^{n+1})$ as *n-cocycles*, and the elements of $\mathrm{Im}(\partial^n)$ as *n-coboundaries*

Remark 6.2.5 This calculation shows that one has natural abelian group isomorphisms

$$\mathrm{Ext}^n_{[\![RG]\!]}(R, A) \cong \mathrm{Ext}^n_{[\![\widehat{\mathbf{Z}}G]\!]}(\widehat{\mathbf{Z}}, A)$$

for all $[\![RG]\!]$-modules A. The role of the ring R is important only in the sense that $H^n(G, A) = \mathrm{Ext}^n_{[\![RG]\!]}(R, A)$ is a discrete R-module. Because of this, we shall often restrict ourselves to cohomology groups $H^n(G, A)$ of G with coefficients in $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$.

6.3 Homology with Coefficients in PMod($[\![RG]\!]$)

We turn our attention next to homology groups. Let G be a profinite group, R a commutative profinite ring and let B be a profinite right $[\![RG]\!]$-module. Define the *n-th homology group $H_n(G,B)$ of G with coefficients in B* by the formula

$$H_n(G,B) = \mathrm{Tor}_n^{[\![RG]\!]}(B,R).$$

Using the definition of $\mathrm{Tor}_n^{[\![RG]\!]}(B,R)$ as the n-th left derived functor of $-\widehat{\otimes}_{[\![RG]\!]} R$, one can make an explicit computation of $H_n(G,B)$ using, for example, the free resolution (1):

Theorem 6.3.1 *$H_n(G,B)$ is the n-th homology group of the chain complex*

$$\cdots \longrightarrow B\,\widehat{\otimes}_{[\![RG]\!]}\, L_{n+1} \longrightarrow B\,\widehat{\otimes}_{[\![RG]\!]}\, L_n \xrightarrow{\partial_n} \cdots \longrightarrow B\,\widehat{\otimes}_{[\![RG]\!]}\, L_0 \longrightarrow 0.$$

We refer to the elements in $\mathrm{Ker}(\partial_n)$ as *n-cycles* , and to those in $\mathrm{Im}(\partial_{n+1})$ as *n-boundaries.*

In particular, this theorem says that

$$H_0(G,B) = \mathrm{Tor}_0^{[\![RG]\!]}(B,R) = B\,\widehat{\otimes}_{[\![RG]\!]}\, R.$$

To give a more suggestive (and often useful) description of $H_0(G,B)$, we proceed as in the case of abstract groups. We denote the usual augmentation ideal of the abstract group $[RG]$ by (IG); that is, (IG) is the kernel of the ring homomorphism (the abstract augmentation map) $[RG] \longrightarrow R$ defined by $g \mapsto 1$, for all $g \in G$ (see, e.g., Mac Lane [1963], p. 104). Define the *augmentation ideal* $(\!(IG)\!) = (\!(I_R G)\!)$ of the complete ring $[\![RG]\!]$ to be the kernel of the continuous ring homomorphism (the augmentation map)

$$\varepsilon : [\![RG]\!] \longrightarrow R$$

given by $\varepsilon(g) = 1$ for every $g \in G$ (note that ε is the inverse limit of the abstract augmentation maps $[(R/L)(G/U)] \longrightarrow R/L$, where U ranges over the open normal subgroups of G and L over the open ideals of R; so, indeed ε is a continuous ring homomorphism).

Lemma 6.3.2 *Let G be a profinite group, R a profinite ring and $(\!(IG)\!) = (\!(I_R G)\!)$ the augmentation ideal of the complete group algebra $[\![RG]\!]$. Then*

(a)

$$(\!(IG)\!) = \varprojlim I(G/U),$$

where U ranges over all open normal subgroups of G.

(b) $(\!(IG)\!)$ *is a free R-module on the pointed topological space*

$$G - 1 = \{x - 1 \mid x \in G\},$$

where 0 is the distinguished point of $G-1$.

(c) *If T is a profinite subspace generating G such that $1 \in T$, then $(\!(IG)\!)$ is generated by the pointed space $T-1 = \{t-1 \mid t \in T\}$, as an $[\![RG]\!]$-module.*

Proof. Part (a) follows from Proposition 2.2.4 and the fact that, by definition, $[\![RG]\!] = \varprojlim [R(G/U)]$.

To prove part (b), let us assume first that G is finite. In that case we must show that the set $\{x-1 \mid 1 \neq x \in G\}$ is an R-basis of (IG). This set is obviously R-linearly independent. Furthermore it generates (IG), for consider $\alpha \in (IG)$, say $\alpha = \sum_{x\in G} \alpha_x x$; then $\sum_{x\in G} \alpha_x = 0$; therefore $\sum_{x\in G} \alpha_x x = \sum_{x\in G} \alpha_x (x-1)$, proving the assertion. If G is infinite, the result follows from this, Proposition 5.2.2 and part (a).

In the proof of (c), we may assume again by part (a), that G is finite. Observe that if $x, y \in G$, then

$$xy - 1 = x(y-1) + (x-1) \quad \text{and} \quad x^{-1} - 1 = -x^{-1}(x-1).$$

Since every element x in G can be expressed in the form $x = t_1^{e_1} \cdots t_r^{e_r}$, ($t_i \in T$, $e_i = \pm 1$), one deduces that every element of the form $x-1$ belongs to the $[RG]$-submodule generated by $T-1$; hence the result. □

To compute $H_0(G,B) = B \widehat{\otimes}_{[\![RG]\!]} R$, consider the short exact sequence

$$0 \longrightarrow (\!(IG)\!) \longrightarrow [\![RG]\!] \longrightarrow R \longrightarrow 0.$$

Since $B \widehat{\otimes}_{[\![RG]\!]} -$ is a right exact functor (see Proposition 5.5.3), the sequence

$$B \widehat{\otimes}_{[\![RG]\!]} (\!(IG)\!) \longrightarrow B \widehat{\otimes}_{[\![RG]\!]} [\![RG]\!] \longrightarrow B \widehat{\otimes}_{[\![RG]\!]} R \longrightarrow 0$$

is exact. After identifying $B \widehat{\otimes}_{[\![RG]\!]} [\![RG]\!]$ with B (see Proposition 5.5.3), and using Lemma 6.3.2, we obtain the following lemma.

Lemma 6.3.3

$$H_0(G,B) \cong B/B(\!(IG)\!) = B/\overline{\langle bg - b \mid b \in B, g \in G\rangle} \stackrel{def}{=} B_G.$$

Furthermore, this isomorphism is natural on the variable B.

Proof. The isomorphism has been already established. The naturality of this isomorphism on the variable B is a consequence of the commutativity of the diagram

$$\begin{array}{ccccccc}
B \widehat{\otimes}_{[\![RG]\!]} (\!(IG)\!) & \longrightarrow & B \widehat{\otimes}_{[\![RG]\!]} [\![RG]\!] & \longrightarrow & B \widehat{\otimes}_{[\![RG]\!]} R & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
B' \widehat{\otimes}_{[\![RG]\!]} (\!(IG)\!) & \longrightarrow & B' \widehat{\otimes}_{[\![RG]\!]} [\![RG]\!] & \longrightarrow & B' \widehat{\otimes}_{[\![RG]\!]} R & \longrightarrow & 0,
\end{array}$$

where the vertical maps are induced by a homomorphism $B \longrightarrow B'$ of $[\![RG]\!]$-modules. □

Therefore, we have the following explicit characterization of the homology functor $\mathbf{H}_\bullet(G,-)$ (see Proposition 6.1.9).

Proposition 6.3.4 $\{H_n(G,-)\}_{n\in\mathbf{N}}$ *is the sequence of left derived functors of the functor $B\mapsto B_G$ from $\mathbf{PMod}(\llbracket RG\rrbracket^{op})$ to $\mathbf{PMod}(R)$. In other words, this sequence is the unique sequence of covariant functors from $\mathbf{PMod}(\llbracket RG\rrbracket^{op})$ to $\mathbf{PMod}(R)$ such that*

(a) $H_0(G,B)=B_G$ *(as functors on $\mathbf{PMod}(\llbracket RG\rrbracket^{op})$),*
(b) $H_n(G,P)=0$ *for every projective profinite right $\llbracket RG\rrbracket$-module P and $n\geq 1$.*
(c) *For each short exact sequence $0\longrightarrow B_1\longrightarrow B_2\longrightarrow B_3\longrightarrow 0$ in $\mathbf{PMod}(\llbracket RG\rrbracket^{op})$, there exist connecting homomorphisms*

$$\delta: H_{n+1}(G,B_3)\longrightarrow H_n(G,B_1),$$

for all $n\geq 0$, such that the sequence

$$\begin{aligned}\cdots\to H_1(G,B_2)\to H_1(G,B_3)&\xrightarrow{\delta} H_0(G,B_1)\\ \to H_0(G,B_2)\to H_0(G,B_3)&\to 0\end{aligned}$$

is exact; and
(d) *For every commutative diagram*

$$\begin{array}{ccccccccc}0 & \longrightarrow & B_1 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & 0\\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & B_1' & \longrightarrow & B_2' & \longrightarrow & B_3' & \longrightarrow & 0\end{array}$$

in $\mathbf{PMod}(\llbracket RG\rrbracket^{op})$ with exact rows, the diagram

$$\begin{array}{ccc}H_{n+1}(G,B_3) & \xrightarrow{\delta} & H_n(G,B_1)\\ {\scriptstyle H_{n+1}(G,\gamma)}\downarrow & & \downarrow{\scriptstyle H_n(G,\alpha)}\\ H_{n+1}(G,B_3') & \xrightarrow{\delta} & H_n(G,B_1')\end{array}$$

commutes for every $n\geq 0$.

We wish to clarify now what is the role of the ring R in the computation of homology groups.

Lemma 6.3.5 *Let G be a profinite group, R a profinite ring and B a profinite right $\llbracket RG\rrbracket$-module. Then there is a natural isomorphism of abelian groups*

$$\mathrm{Tor}_n^{\llbracket RG\rrbracket}(B,R)\cong \mathrm{Tor}_n^{\llbracket\widehat{\mathbf{Z}}G\rrbracket}(B,\widehat{\mathbf{Z}}).$$

Proof. Put $\Lambda = [\![\widehat{\mathbf{Z}}G]\!]$. Consider a free Λ-resolution of $\widehat{\mathbf{Z}}$ (for example (2))

$$\cdots \to [\![\Lambda X_n]\!] \to [\![\Lambda X_{n-1}]\!] \to \cdots \to [\![\Lambda X_0]\!] \to \widehat{\mathbf{Z}} \to 0, \tag{5}$$

where each X_n is a profinite space. Since each $[\![\Lambda X_n]\!]$ is automatically a free $\widehat{\mathbf{Z}}$-module, (5) is a projective $\widehat{\mathbf{Z}}$-resolution of $\widehat{\mathbf{Z}}$ as well. Furthermore, this resolution is $\widehat{\mathbf{Z}}$-*split*, that is, each term of the sequence is the direct sum of the image of the previous map and the kernel of the next map as $\widehat{\mathbf{Z}}$-modules (this is a consequence of the $\widehat{\mathbf{Z}}$-projectivity of each term of the sequence). One easily deduces from this that tensoring (5) with R over $\widehat{\mathbf{Z}}$ yields an exact sequence

$$\cdots \to R \widehat{\otimes}_{\widehat{\mathbf{Z}}} [\![\Lambda X_n]\!] \to \cdots \to R \widehat{\otimes}_{\widehat{\mathbf{Z}}} [\![\Lambda X_0]\!] \to R \widehat{\otimes}_{\widehat{\mathbf{Z}}} \widehat{\mathbf{Z}} \cong R \to 0. \tag{6}$$

Next observe that (6) is an $[\![RG]\!]$-free resolution of R. Indeed, if X is a profinite space,

$$R \widehat{\otimes}_{\widehat{\mathbf{Z}}} [\![\Lambda X]\!] = \varprojlim R \widehat{\otimes}_{\widehat{\mathbf{Z}}} [\![[\widehat{\mathbf{Z}}(G/U)]Y_i]\!],$$

where U ranges over the open normal subgroups of G, and where $X = \varprojlim Y_i$, with each Y_i finite. By Proposition 5.5.3(d),

$$R \widehat{\otimes}_{\widehat{\mathbf{Z}}} [\![[\widehat{\mathbf{Z}}(G/U)]Y_i]\!] = R \otimes_{\widehat{\mathbf{Z}}} [\![[\widehat{\mathbf{Z}}(G/U)]Y_i]\!] = [\![[R(G/U)]Y_i]\!];$$

thus $R \widehat{\otimes}_{\widehat{\mathbf{Z}}} [\![\Lambda X]\!] = [\![[\![RG]\!]X]\!]$, a free $[\![RG]\!]$-module.

Now suppose that B is a profinite right $[\![RG]\!]$-module. Then there exists a natural isomorphism of profinite abelian groups

$$B \widehat{\otimes}_{[\![RG]\!]} (R \widehat{\otimes}_{\widehat{\mathbf{Z}}} [\![\Lambda X_n]\!]) \cong B \widehat{\otimes}_{[\![\widehat{\mathbf{Z}}G]\!]} [\![\Lambda X_n]\!]$$

given by

$$b \widehat{\otimes} (r \widehat{\otimes} d) \mapsto br \widehat{\otimes} d \quad (b \in B, r \in R, d \in [\![\Lambda X_n]\!]).$$

Thus the result. $\square$

Because of this lemma, we shall often state our results only for homology groups $H_n(G,B)$, where B is a profinite right $[\![\widehat{\mathbf{Z}}G]\!]$-module.

We end this section by establishing a duality relationship between homology and cohomology groups.

Proposition 6.3.6 *Let G be a profinite group and let B be a profinite right $[\![\widehat{\mathbf{Z}}G]\!]$-module. Then*

$$H_n(G,B) \quad \text{and} \quad H^n(G,B^*) \quad (n \in \mathbf{N})$$

are Pontryagin dual, where B^* denotes the Pontryagin dual of B (see Section 5.1).

Proof. We must show that $H_n(G,B) \cong H^n(G,B^*)^*$. In fact we shall show that $\{H_n(G,-)\}_{n\in\mathbf{N}}$ and $\{H^n(G,-^*)^*\}_{n\in\mathbf{N}}$ are isomorphic homological functors from $\mathbf{Mod}([\![\widehat{\mathbf{Z}}G]\!]^{op})$ to $\mathbf{Mod}(\widehat{\mathbf{Z}})$.

That $\{H^n(G,-^*)^*\}_{n\in\mathbf{N}}$ is a homological functor follows from the following facts:

(1) $\{H^n(G,-)\}_{n\in\mathbf{N}}$ is a cohomological functor from $\mathbf{Mod}([\![\widehat{\mathbf{Z}}G]\!])$ to $\mathbf{Mod}(\widehat{\mathbf{Z}})$, and

(2) $\mathrm{Hom}(-,\mathbf{Q}/\mathbf{Z})$ is an exact functor, since $\mathbf{Q}/\mathbf{Z}$ is an injective discrete $\widehat{\mathbf{Z}}$-module (to see the latter assertion observe that the discrete $\widehat{\mathbf{Z}}$-modules are precisely the torsion abelian groups; on the other hand, $\mathbf{Q}/\mathbf{Z}$ is injective as an abelian group since it is divisible).

Therefore, it suffices to prove that both sequences are coeffaceable and isomorphic in dimension 0 (see Lemma 6.1.4). If P is a projective profinite $[\![\widehat{\mathbf{Z}}G]\!]$-module, then P^* is an injective discrete $[\![\widehat{\mathbf{Z}}G]\!]$-module; so $H^n(G,P^*) = 0$ for $n \geq 1$; hence $\{H^n(G,-^*)^*\}_{n\in\mathbf{N}}$ is coeffaceable. Finally we must show that $H_0(G,B)$ and $H^0(G,B^*)^*$ are isomorphic as functors on the second variable. Now,

$$\begin{aligned} H^0(G,B^*)^* &= (\mathrm{Hom}_{[\![\widehat{\mathbf{Z}}G]\!]}(\widehat{\mathbf{Z}}, \mathrm{Hom}_{\widehat{\mathbf{Z}}}(B,\mathbf{Q}/\mathbf{Z}))^* \\ &\cong \mathrm{Hom}_{\widehat{\mathbf{Z}}}(B \mathbin{\widehat{\otimes}}_{[\![\widehat{\mathbf{Z}}G]\!]} \widehat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z})^* \cong B \mathbin{\widehat{\otimes}}_{[\![\widehat{\mathbf{Z}}G]\!]} \widehat{\mathbf{Z}} = H_0(G,B) \end{aligned}$$

(the first isomorphism follows from Proposition 5.5.4, and the second is just Pontryagin duality). □

The above proposition allows us to prove general results for cohomology (respectively, homology) groups of a group G, obtaining automatically corresponding results for homology (respectively, cohomology) groups, by duality.

6.4 Cohomology Groups with Coefficients in DMod(G)

Let G be a profinite group. The definition given in Section 6.2 for the cohomology groups of G is valid for coefficient modules A in $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$ (or more generally, in $\mathbf{DMod}([\![RG]\!])$). In this section we shall extend this definition to include any coefficient module from $\mathbf{DMod}(G)$. We do this in a way that makes it irrelevant whether A is in $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$ or in $\mathbf{DMod}(G)$.

Let G be a profinite group and let A be a discrete G-module. Define a cochain complex $\mathbf{C}(G,A)$:

$$0 \to C^0(G,A) \to C^1(G,A) \to \cdots \to C^n(G,A) \xrightarrow{\partial^{n+1}} C^{n+1}(G,A) \to \cdots,$$

where $C^n(G,A)$ is the abelian group of all continuous functions

$$f : G \times \overset{n+1}{\cdots} \times G \longrightarrow A \tag{7}$$

such that $f(xx_0, \ldots, xx_n) = xf(x_0, \ldots, x_n) \quad (x, x_0, \ldots, x_n \in G)$, and ∂^{n+1} is defined by the formula (4), i.e.,

$$(\partial^{n+1} f)(x_0, x_1, \ldots, x_{n+1}) = \sum_{i=0}^{n+1} (-1)^i f(x_0, \ldots, \hat{x}_i, \ldots x_{n+1}), \tag{8}$$

where $x_0, x_1, \ldots, x_{n+1} \in G$.

For simplicity, we often drop the superindices and write ∂ rather than ∂^n if there is no danger of confusion.

Definition 6.4.1 *Let G and A be as above. Then the n-th cohomology group of G with coefficients in A is defined as the n-th cohomology group of the cochain complex* (7), *i.e.,*

$$H^n(G, A) = \mathrm{Ker}(\partial^{n+1})/\mathrm{Im}(\partial^n).$$

As previously, the elements in $\mathrm{Ker}(\partial^{n+1})$ are called *n-cocycles*, and those in $\mathrm{Im}(\partial^n)$, *n-coboundaries.*

According to Theorem 6.2.4, this is consistent with the definition of the cohomology groups with coefficient modules A in $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$. This justifies formally our approach; there is however another more substantial reason to justify this definition. Indeed, as we shall see later, with Definition 6.4.1 each $H^n(G, A)$ becomes a functor on the second variable; in fact (see Section 6.6) $\{H^n(G, A)\}_{n \in \mathbf{N}}$ is the sequence of right derived functors of the left exact functor

$$-^G : \mathbf{DMod}(G) \longrightarrow \mathfrak{A},$$

where $\mathfrak{A}$ is the category of abelian groups : if A is a discrete G-module, then $A^G = \{a \in A \mid ga = a, \ \forall g \in G\}$ is in fact a "trivial" G-module in the sense that the natural action of G on A^G is the trivial one; see Section 5.8 where A^G was defined for $[\![RG]\!]$-modules. This is plausible in principle since $\mathbf{DMod}(G)$ has enough injectives. Also, in this process we shall make explicit some maps, like the connecting homomorphisms involved in the cohomological functor $\{H^n(G, A)\}_{n \in \mathbf{N}}$ (defined either in $\mathbf{DMod}(G)$ or in $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$, the latter being a restriction of the former).

Exercise 6.4.2 Let G be a profinite group and R a commutative profinite ring. Assume that A is a discrete left G-module (respectively, $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$). Let $\tilde{C}^n(G, A)$ denote the group of all continuous functions $f : G \times \overset{n}{\cdots} \times G \longrightarrow A$. Define a cochain complex $\tilde{\mathbf{C}}(G, A)$:

$$0 \to \tilde{C}^0(G, A) \to \cdots \to \tilde{C}^n(G, A) \xrightarrow{\tilde{\partial}^{n+1}} \tilde{C}^{n+1}(G, A) \to \cdots,$$

where

$$(\tilde{\partial}^{n+1} f)(x_1, \ldots, x_{n+1}) = x_1 f(x_2, \ldots, x_{n+1}) + \sum_{i=1}^{n} (-1)^i f(x_1, \ldots, x_i x_{i+1}, \ldots, x_{n+1}) + (-1)^{n+1} f(x_1, \ldots, x_n).$$

Prove that $H^n(G,A)$ (see Definition 6.4.1) is the n-th cohomology group of this complex.

6.5 The Functorial Behavior of $H^n(G,A)$ and $H_n(G,A)$

Let $\varphi : G \longrightarrow G'$ be a continuous homomorphism of profinite groups. Let $A \in \mathbf{DMod}(G)$, $A' \in \mathbf{DMod}(G')$, and let $f : A' \longrightarrow A$ be a group homomorphism. As in Section 5.1, we say that φ and f are *compatible* maps if

$$f(\varphi(x)a') = xf(a'), \quad (x \in G, \quad a' \in A'),$$

i.e., if f is a G-homomorphism when A' is considered as a G-module by means of the action $xa' \stackrel{def}{=} \varphi(x)a'$, $(x \in G,\ a' \in A')$.

Example 6.5.1 Let $N \supset L \supset K$ be Galois extensions of fields. Then the natural projection and injection

$$\pi : G_{N/K} \longrightarrow G_{L/K} \quad \text{and} \quad i : L^* \hookrightarrow N^*,$$

respectively, are easily seen to be compatible (see Example 5.3.2).

A pair of compatible maps φ, f as above, induces homomorphisms

$$(\varphi, f) : C^n(G', A') \longrightarrow C^n(G, A) \quad (n \geq 0)$$

given by

$$[(\varphi, f)\sigma](x_0, \ldots, x_n) = f(\sigma(\varphi(x_0), \ldots, \varphi(x_n))) \quad (\sigma \in C^n(G', A'), x_i \in G).$$

In fact (φ, f) is a map of cochain complexes, i.e.,

$$\begin{array}{ccc} C^n(G', A') & \xrightarrow{\partial^{n+1}} & C^{n+1}(G', A') \\ \downarrow{\scriptstyle(\varphi,f)} & & \downarrow{\scriptstyle(\varphi,f)} \\ C^n(G, A) & \xrightarrow{\partial^{n+1}} & C^{n+1}(G, A) \end{array}$$

commutes for $n \geq 0$. From this one easily defines homomorphisms

$$(\varphi, f)^n : H^n(G', A') \longrightarrow H^n(G, A)$$

of the cohomology groups.

The maps $(\varphi, f)^n$ that we have just constructed behave functorially in the following sense. Let G_i be profinite groups and let $A_i \in \mathbf{DMod}(G_i)$ $(i = 1, 2, 3)$. Assume that

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3$$

and

$$A_1 \xleftarrow{f_1} A_2 \xleftarrow{f_2} A_3$$

are continuous homomorphisms and abelian group homomorphisms, respectively, such that the pairs φ_1 and f_1, and φ_2 and f_2 are compatible. Then one checks that $\varphi_2\varphi_1$ and $f_2 f_1$ are compatible, and

$$(\varphi_2\varphi_1, f_2 f_1)^n = (\varphi_1, f_1)^n \circ (\varphi_2, f_2)^n.$$

Moreover, if $\varphi_1 : G_1 \longrightarrow G_1$ and $f_1 : A_1 \longrightarrow A_1$ are identity maps, so is $(\varphi_1, f_1)^n$. In particular, we have established the following result.

Proposition 6.5.2 *$H^n(G,-)$ is a functor from the category* $\mathbf{DMod}(G)$ *to the category $\mathfrak{A}$ of abelian groups $(n \geq 0)$.*

The Inflation Map

Let K be a closed normal subgroup of a profinite group G, and let $A \in \mathbf{DMod}(G)$. Then A^K becomes a G/K-module in a natural way:

$$(xK)(a) = xa, \quad (x \in G, a \in A^K).$$

It is clear that the projection $G \longrightarrow G/K$ and the inclusion $A^K \longrightarrow A$ are compatible maps. Hence for each n, they induce homomorphisms

$$\mathrm{Inf} = \mathrm{Inf}_G^{G/K} : H^n(G/K, A^K) \longrightarrow H^n(G,A)$$

which are called *inflations*. Explicitly,

$$\mathrm{Inf} : H^0(G/K, A^K) = (A^K)^{G/K} \longrightarrow H^0(G,A) = A^G$$

is the identity mapping. Assume $n > 0$, and let $\sigma \in C^n(G/K, A^K)$ represent an element $\bar{\sigma}$ of $H^n(G/K, A^K)$, i.e., $\sigma : (G/K)^{n+1} \longrightarrow A^K$ is a (continuous) n-cocycle. Then $\mathrm{Inf}(\bar{\sigma})$ is represented by the continuous n-cocycle

$$\rho : G^{n+1} \longrightarrow A$$

given by

$$\rho(x_0, \ldots, x_n) = \sigma(x_0 K, \ldots, x_n K).$$

From this definition it is straightforward to check the following proposition.

Proposition 6.5.3

(a) *Let K be a normal closed subgroup of a profinite group G. Let $f : A \longrightarrow B$ be a map of G-modules. Then f induces a G/K-homomorphism $f^K : A^K \longrightarrow B^K$, and the diagram*

$$\begin{array}{ccc} H^n(G/K, A^K) & \xrightarrow{(\mathrm{id}, f^K)^n} & H^n(G/K, B^K) \\ \Big\downarrow \mathrm{Inf} & & \Big\downarrow \mathrm{Inf} \\ H^n(G, A) & \xrightarrow{(\mathrm{id}, f)^n} & H^n(G, B) \end{array}$$

commutes. In other words, $\mathrm{Inf} : H^n(G/K, -^K) \longrightarrow H^n(G, -)$ *is a morphism of functors for each* $n \geq 0$.

(b) *Let* G *and* K *be as in part* (a). *Let* $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ *be a short exact sequence of* G*-modules and assume that the corresponding sequence* $0 \longrightarrow A^K \longrightarrow B^K \longrightarrow C^K \longrightarrow 0$ *of* G/K*-modules is also exact. Then* Inf *commutes with the corresponding connecting homomorphisms, that is, for each natural number* n *we have a commutative diagram*

$$\begin{array}{ccc} H^n(G/K, C^K) & \xrightarrow{\delta} & H^{n+1}(G/K, A^K) \\ \Big\downarrow \mathrm{Inf} & & \Big\downarrow \mathrm{Inf} \\ H^n(G, C) & \xrightarrow{\delta} & H^{n+1}(G, A). \end{array}$$

(c) *If* $G \longrightarrow G_1$ *and* $G_1 \longrightarrow G_2$ *are surjective continuous homomorphisms of profinite groups, then*

$$\mathrm{Inf}_G^{G_1} \mathrm{Inf}_{G_1}^{G_2} = \mathrm{Inf}_G^{G_2}.$$

Let I be a directed poset and let $\{G_i, \varphi_{ij}, I\}$ be an inverse system over I of profinite groups. Let $\{A_i, f_{ij}, I\}$ be a direct system over I of abelian groups, where each A_i is a G_i-module such that, for each pair $i \succeq j$ in I, the maps

$$\varphi_{ij} : G_i \longrightarrow G_j \quad \text{and} \quad f_{ji} : A_j \longrightarrow A_i$$

are compatible. Then, for each n, we obtain in a natural way direct systems over I

$$\{C^n(G_i, A_i)\}_{i \in I} \quad \text{and} \quad \{H^n(G_i, A_i)\}_{i \in I}.$$

Let

$$G = \varprojlim_{i \in I} G_i \quad \text{and} \quad A = \varinjlim_{i \in I} A_i.$$

Denote by $\varphi_i : G \longrightarrow G_i$ and $f_i : A_i \longrightarrow A$ the corresponding canonical homomorphisms. Then A can be considered as a G-module in the following manner: given $a \in A$ and $x \in G$, then for some $i \in I$ and $a_i \in A_i$ one has $f_i(a_i) = a$; define $xa \stackrel{def}{=} f_i[(\varphi_i(x))a_i]$. This is a well defined continuous action of G on A.

Lemma 6.5.4 *Under the above assumptions one has*

(a)

$$C^n(G, A) \cong \varinjlim_{i \in I} C^n(G_i, A_i) \quad (n = 0, 1, \ldots).$$

Moreover these isomorphisms commute with the operators ∂ *given by formula* (8) *in the following sense*: *for each* $i \in I$ *the diagram*

$$\begin{array}{ccc} C^n(G_i, A_i) & \xrightarrow{\partial^{n+1}} & C^{n+1}(G_i, A_i) \\ \downarrow \cong & & \downarrow \cong \\ C^n(G, A) & \xrightarrow{\partial^{n+1}} & C^{n+1}(G, A) \end{array}$$

commutes.

(b) $C^n(G, -)$ *is an exact functor on the category* $\mathbf{DMod}(G)$.

Proof. Fix n. For each $i \in I$ define a homomorphism

$$\Psi_{ni} : C^n(G_i, A_i) \longrightarrow C^n(G, A)$$

as follows. Let $\sigma_i \in C^n(G_i, A_i)$, then put $\Psi_{ni}(\sigma_i) = f_i \sigma_i \varphi_i$. The homomorphisms Ψ_{ni} are compatible with the canonical homomorphisms

$$C^n(G_i, A_i) \longrightarrow C^n(G_j, A_j) \quad (i \preceq j).$$

Hence they induce homomorphisms

$$\Psi_n : \varinjlim_{i \in I} C^n(G_i, A_i) \longrightarrow C^n(G, A).$$

The commutativity of the homomorphisms Ψ_n with the operators ∂ follow immediately from these definitions and formula (8).

The proof that each Ψ_n is an isomorphism is very similar to the proof of Lemma 5.1.4(a), and we leave the details to the reader.

(b) Let $\mathcal{U}$ be the set of all open normal subgroups of G. Note that $\{G/U\}_{U \in \mathcal{U}}$ is an inverse system of finite groups, $\{A^U\}_{U \in \mathcal{U}}$ a direct system of abelian groups and A^U is a G/U-module by means of the action $(gU)a = ga$. The canonical homomorphisms $G/U \longrightarrow G/V$ and $A^U \longleftarrow A^V$ $(U \leq V)$, are compatible. So by part (a),

$$C^n(G, A) \cong \varinjlim_{U \in \mathcal{U}} C^n(G/U, A^U).$$

Now, since $\varinjlim$ is an exact functor on abelian groups (see Proposition 1.2.6), then in the proof of (b) we may assume that G is finite. For finite G,

$$C^n(G, -) = \operatorname{Hom}_{[\mathbf{Z}G]}(F, -),$$

where F is the free $[\mathbf{Z}G]$-module on the set G^n. Hence $C^n(G, -)$ is exact. □

We can now translate this information to cohomology.

Proposition 6.5.5 *For each* $n \geq 0$

$$H^n(G,A) \cong \varinjlim_I H^n(G_i,A_i).$$

Proof. Since $\varinjlim$ is an exact functor on the category of abelian groups (see Proposition 1.2.6), one has

$$\varinjlim_I H^n(G_i,A_i) \cong H^n\Big(\varinjlim_I \mathbf{C}^\bullet(G_i,A_i)\Big),$$

where the cochain complexes $\mathbf{C}^\bullet(G_i,A_i)$ form a direct system by means of the maps

$$g_{ij} = (\varphi_{ji}, f_{ij}) : C^n(G_i,A_i) \longrightarrow C^n(G_j,A_j),$$

given by $g_{ij}(\sigma_i) = f_{ij}\sigma_i\varphi_{ji}$ $(\sigma_i \in C^n(G_i,A_i),\ j \succeq i)$. Note that the maps g_{ij} determine a map of cochain complexes

$$\mathbf{C}^\bullet(G_i,A_i) \longrightarrow \mathbf{C}^\bullet(G_j,A_j)$$

since they commute with the coboundary operators ∂^n. Hence, to prove our assertion it suffices to show the existence of isomorphisms

$$\varinjlim_{i\in I} C^n(G_i,A_i) \cong C^n(G,A),$$

$n \geq 0$, commuting with the coboundary maps ∂^n. This is the content of Lemma 6.5.4. □

Corollary 6.5.6 *Let* G *be a profinite group and* $A \in \mathbf{DMod}(G)$*. Then*

(a)
$$H^n(G,A) = \varinjlim_{U\in\mathcal{U}} H^n(G/U,A^U)$$

where $\mathcal{U}$ *is the collection of all open normal subgroups of* G*.*

(b)
$$H^n(G,A) = \varinjlim_{A'} H^n(G,A'),$$

where A' *runs through the finitely generated* G*-submodules of* A*.*

(c) *Suppose* $A = \bigoplus_{i\in I} A_i$ *is a direct sum of* G*-submodules of* A*. Then*

$$H^n(G,A) = \bigoplus_{i\in I} H^n(G,A_i) \quad \text{for all } n \geq 0.$$

Proof. (a) As indicated in the proof of part (b) of Lemma 6.5.4,

$$C^n(G,A) \cong \varinjlim_{U\in\mathcal{U}} C^n(G/U, A^U).$$

Furthermore, by Lemma 6.5.4(a) these isomorphisms commute with ∂ (see formula (8)). Since $\varinjlim$ is an exact functor, we obtain from Lemma 6.5.4(a) that

$$\begin{aligned} H^n(G,A) = H^n(\mathbf{C}^\bullet(G,A)) &= H^n(\varinjlim_{U\in\mathcal{U}} \mathbf{C}^\bullet(G/U, A^U)) \\ &= \varinjlim_{U\in\mathcal{U}} H^n(\mathbf{C}^\bullet(G/U,A^U)) = \varinjlim_{U\in\mathcal{U}} H^n(G/U, A^U). \end{aligned}$$

(b) This follows from the proposition above since $A = \varinjlim A'$.

(c) $A = \varinjlim_J A_J$, where $A_J = \bigoplus_{j\in J} A_j$, and J ranges over all finite subsets of I. Hence the result follows from Proposition 6.5.5 and the fact that each $H^n(G,-)$ is an additive functor. □

We turn now to homology. The functorial behavior of $H_n(G,B)$ can be deduced by duality from the behavior of $H^n(G,B^*)$ (see Proposition 6.3.6). In detail, consider a homomorphism of profinite groups $\varphi : G \longrightarrow G'$ and a homomorphism $f : B \longrightarrow B'$ of profinite abelian groups; assume that B is a profinite right G-module, B' a profinite right G'-module, and that the maps φ and f are compatible (i.e., $f(bx) = f(b)\varphi(x)$, for all $x \in G$, $b \in B$). Then φ and the dual map $f^* : B'^* \longrightarrow B^*$ are compatible; hence, as we have seen above, for each natural number n, there exists a corresponding homomorphism

$$(\varphi, f)^n : H^n(G, B^*) \longrightarrow H^n(G', B'^*).$$

The dual of this map is the desired continuous homomorphism for the homology groups

$$(\varphi, f)_n = ((\varphi, f)^n)^* : H_n(G,B) \longrightarrow H_n(G', B').$$

Using Theorem 6.3.1, there is an obvious way of describing explicitly the maps $(\varphi, f)_n$ in terms of chains; we leave this to the reader.

We term the dual of inflation, *coinflation*. It is defined as follows. Let K be a closed normal subgroup of a profinite group G, and let $\varphi : G \longrightarrow G/K$ be the canonical homorphism. Let B be a profinite right $[\![\widehat{\mathbf{Z}}G]\!]$-module, and consider the canonical projection $f : B \longrightarrow B_K = B/B(\!(IK)\!)$ (see Lemma 6.3.3). Then φ and f are compatible maps; hence they induce continuous homorphisms of homology groups:

$$\mathrm{Coinf} = \mathrm{Coinf}^G_{G/K} : H_n(G,B) \longrightarrow H_n(G/K, B_K) \quad (n \geq 0),$$

called the coinflation maps.

To get dual results to Proposition 6.5.5 and Corollary 6.5.6, we need some notation first. Let

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

be a profinite group expressed as an inverse limit of an inverse system $\{G_i, \varphi_{ij}, I\}$ of profinite groups. Assume that

$$B = \varprojlim_{i \in I} B_i$$

is a profinite abelian group expressed as an inverse limit of an inverse system $\{B_i, f_{ij}, I\}$ of profinite abelian groups over the same indexing poset I. Suppose, in addition, that each B_i has the structure of a right $[\![\widehat{\mathbf{Z}}G_i]\!]$-module and that φ_{ij} and f_{ij} are compatible maps for each pair $i, j \in I$ such that $i \succeq j$. Then we have

Proposition 6.5.7 *For each* $n \geq 0$,

$$H_n(G, B) \cong \varprojlim_{I} H_n(G_i, B_i).$$

The first part of the following corollary is just the dual of Lemma 5.3.1(c); the second part follows from the proposition above.

Corollary 6.5.8 *Let G be a profinite group and A a profinite right $[\![\widehat{\mathbf{Z}}G]\!]$-module. Then*

(a)

$$B = \varprojlim_{U \in \mathcal{U}} B_U,$$

where $\mathcal{U}$ is the collection of open normal subgroups of G.

(b)

$$H_n(G, B) = \varprojlim_{U \in \mathcal{U}} H_n(G/U, B_U).$$

6.6 $H^n(G, A)$ as Derived Functors on DMod(G)

As announced in Section 6.4, we shall prove here that the sequence of functors $\{H^n(G, -)\}_{n \in \mathbf{N}}$ on $\mathbf{DMod}(G)$ is a positive effaceable cohomological functor, in fact it is the sequence of right derived functors of the functor $A \mapsto A^G$ that maps a discrete G-module A to its submodule of fixed points. The proofs here are necessarily computational. On the other hand, since by definition cohomology with coefficients in $\mathbf{DMod}(G)$ includes cohomology with coefficients in $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$, our computations using cochains are valid for all coefficient modules, whether torsion or not.

Lemma 6.6.1 *Let*

$$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$$

be an exact sequence of discrete G-modules and G-homomorphisms. Then there exist canonical homomorphisms (the "connecting homomorphisms")

$$\delta = \delta^n : H^n(G, C) \longrightarrow H^{n+1}(G, A) \quad (n \geq 0)$$

such that the sequence

$$\begin{aligned} 0 \longrightarrow A^G \xrightarrow{\varphi^0} B^G \xrightarrow{\psi^o} C^G \xrightarrow{\delta^o} H^1(G, A) \\ \xrightarrow{\varphi^1} H^1(G, B) \xrightarrow{\psi^1} H^1(G, C) \xrightarrow{\delta^1} H^2(G, A) \xrightarrow{\varphi^2} \cdots \end{aligned}$$

is exact, where the maps φ^n and ψ^n are induced by φ and ψ respectively.

Proof. One way of proving this is to assume first that G is finite. The existence of this exact sequence is well-known in that case (see, e.g., Mac Lane [1963], pages 116 and 97). Since $\varinjlim$ is exact in the category of abelian groups, the result follows from Corollary 6.5.6.

Next, we give a direct proof of this lemma for a general profinite group G. In this proof we indicate an explicit definition of the connecting homomorphisms δ^n. Consider the short exact sequence of cochain complexes induced by φ and ψ:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
\cdots \longrightarrow & & C^n(G, A) & \xrightarrow{\partial} & C^{n+1}(G, A) & & \longrightarrow \cdots \\
 & & \downarrow \varphi & & \downarrow \varphi & & \\
\cdots \longrightarrow & & C^n(G, B) & \xrightarrow{\partial} & C^{n+1}(G, B) & & \longrightarrow \cdots \\
 & & \downarrow \psi & & \downarrow \psi & & \\
\cdots \longrightarrow & & C^n(G, C) & \xrightarrow{\partial} & C^{n+1}(G, C) & & \longrightarrow \cdots \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array}$$

By Lemma 6.5.4, each vertical line is a short exact sequence of abelian groups. For a discrete G-module M, we shall represent an element of $H^n(G, M)$ by $[\mu]$, where $\mu \in C^n(G, M)$ is a cocycle (i.e., $\partial(\mu) = 0$; see the complex (8)).

Let $[\sigma_n] \in H^n(G, C)$; then $\partial(\sigma_n) = 0$. Let $\rho_n \in C^n(G, B)$ with $\psi(\rho_n) = \sigma_n$. Then $0 = \partial\psi(\rho_n) = \psi\partial(\rho_n)$. Hence there exists $\nu_{n+1} \in C^{n+1}(G, A)$ with $\varphi(\nu_{n+1}) = \partial(\rho_n)$. Clearly $\partial(\nu_{n+1}) = 0$. Define

$$\delta([\sigma_n]) = [\nu_{n+1}] \in H^{n+1}(G, A).$$

To see that δ is well defined, assume that also $\rho'_n \in C^n(G, B)$ with $\psi(\rho'_n) = \sigma_n$; let $\nu'_{n+1} \in C^{n+1}(G, A)$ be such that $\varphi(\nu'_{n+1}) = \partial(\sigma'_n)$. We must show that $[\nu'_{n+1}] = [\nu_{n+1}]$. Indeed, since $\psi(\rho'_n - \rho_n) = 0$, there exists $\nu_n \in C^n(G, A)$ with $\varphi(\nu_n) = \rho'_n - \rho_n$; then $\varphi\partial(\nu_n) = \partial(\rho'_n - \rho_n) = \varphi(\nu'_{n+1} - \nu_{n+1})$. Hence $\partial(\nu_n) = \nu'_{n+1} - \nu_{n+1}$, because φ is injective. In other words, $\nu'_{n+1} - \nu_{n+1}$ is a coboundary, i.e., $[\nu'_{n+1}] = [\nu'_{n+1}]$. It is an easy exercise to check that δ is a homomorphism. Moreover, the long sequence in the statement of the lemma is exact. The verification of this requires easy diagram chasing, and we leave most of this verification to the reader. As a sample, we check the exactness at $H^{n+1}(G, A)$. First observe that the definition of δ above implies that $\varphi^{n+1}\delta = 0$; therefore $\mathrm{Im}(\delta) \le \mathrm{Ker}(\varphi^{n+1})$. Conversely, let $[\nu_{n+1}] \in H^{n+1}(G, A)$, where $\nu_{n+1} \in C^{n+1}(G, A)$ is a cocycle, i.e., $\partial(\nu_{n+1}) = 0$. Assume that $\varphi^{n+1}([\nu_{n+1}]) = 0$. This means that $\varphi(\nu_{n+1}) = \partial(\nu_n)$ for some $\nu_n \in C^n(G, B)$. Then, by the definition of δ above, we have that $\delta([\psi(\nu_n)]) = [\nu_{n+1}]$. Thus $\mathrm{Im}(\delta) \ge \mathrm{Ker}(\varphi^{n+1})$. □

We can now characterize in a global way the cohomology groups of a profinite group with coefficients in the category of all discrete G-modules.

Theorem 6.6.2 *The sequence of functors*

$$\{H^n(G, -) : \mathbf{DMod}(G) \longrightarrow \mathfrak{A}\}_{n \ge 0}$$

is the sequence of right derived functors of the functor

$$-^G : \mathbf{DMod}(G) \longrightarrow \mathfrak{A}$$

that sends a discrete G-module A to the abelian group A^G of fixed elements of A.

Proof. Let $A, B \in \mathbf{DMod}(G)$. Then $C^n(G, A \oplus B) = C^n(G, A) \oplus C^n(G, B)$; so $H^n(G, A \oplus B) = H^n(G, A) \oplus H^n(G, B)$, i.e., $H^n(G, -)$ is an additive functor for each $n \ge 0$. By definition of derived functors, we must show that $\{H^n(G, -)\}_{n \ge 0}$ is an effaceable covariant cohomological functor and that $H^0(G, -) \cong -^G$. First we show that it is a cohomological functor. In view of Lemma 6.6.1, it only remains to see that every commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \xrightarrow{\varphi'} & B' & \xrightarrow{\psi'} & C' & \longrightarrow & 0 \end{array}$$

of G-modules and G-homomorphisms, with exact rows, induces a commutative diagram

$$\begin{array}{ccc} H^n(G,C) & \xrightarrow{\delta} & H^{n+1}(G,A) \\ \downarrow & & \downarrow \\ H^n(G,C') & \xrightarrow[\delta']{} & H^{n+1}(G,A') \end{array}$$

for each $n \geq 0$. This follows immediately from the definition of δ and δ' (see the proof of Lemma 6.6.1).

Next observe that

$$H^0(G,G) = \mathrm{Ker}(C^0(G,A) \longrightarrow C^1(G,A)) \cong A^G;$$

moreover this isomorphism determines a natural equivalence of functors.

Finally, it is necessary to prove that the sequence is effaceable, i.e., that $H^n(G,Q) = 0$ for every injective object in $\mathbf{DMod}(G)$ and $n > 0$. Let U be an open normal subgroup of G. It is easy to see that Q^U is an injective G/U-module; hence $H^n(G/U, Q^U) = 0$ (see Proposition 6.2.2). Thus, by Corollary 6.5.6,

$$H^n(G,Q) = \varinjlim_{U} H^n(G/U, Q^U) = 0. \qquad \square$$

Proposition 6.6.3 *Let G be a profinite group and $H \leq_c G$. Then*

$$\{H^n(H,-)\}_{n\in\mathbf{N}}$$

is a universal cohomological functor $\mathbf{DMod}(G) \longrightarrow \mathfrak{A}$.

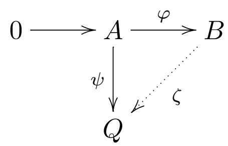
Proof. It is obvious that $\{H^n(H,-)\}_{n\in\mathbf{N}}$ is a cohomological functor from $\mathbf{DMod}(G)$ to $\mathfrak{A}$. To prove universality we must show that $H^n(H,Q) = 0$ if $n > 0$ and Q is injective in $\mathbf{DMod}(G)$ (see Proposition 6.1.2). By Proposition 6.5.5

$$H^n(H,Q) = \varinjlim_{U\in\mathcal{U}} H^n(HU/U, Q^U)$$

($\mathcal{U}$ is the collection of all open normal subgroups of G). Since Q^U is G/U-injective, it will suffice to prove the following lemma. $\square$

Lemma 6.6.4 *Let $H \leq G$ be abstract groups and let Q be an injective abstract G-module, then Q is injective as an abstract H-module.*

Proof. One can adapt the proof of Corollary 5.7.2 to abstract groups. Instead we give a different proof which is completely explicit. Consider a diagram



of H-modules, where φ is a monomorphism. We need an H-homomorphism $\zeta : B \longrightarrow Q$ such that $\zeta\varphi = \psi$.

Construct a new diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & [\mathbf{Z}G] \otimes_{[\mathbf{Z}H]} A & \xrightarrow[\bar\varphi]{} & [\mathbf{Z}G] \otimes_{[\mathbf{Z}H]} B \\ & & \downarrow{\scriptstyle \bar\psi} & \swarrow{\scriptstyle \bar\zeta} & \\ & & Q & & \end{array}$$

of G-modules and G-homomorphisms. The abelian groups $[\mathbf{Z}G] \otimes_{[\mathbf{Z}H]} A$ and $[\mathbf{Z}G] \otimes_{[\mathbf{Z}H]} B$ are considered as G-modules by means of the action $x(r \otimes a) = xr \otimes a$, ($x \in G$, $r \in [\mathbf{Z}H]$, $a \in A$). The G-homorphisms $\bar\varphi$ and $\bar\psi$ are given by

$$\begin{aligned} &\bar\varphi(s \otimes a) = s \otimes \varphi(a), \\ &\bar\psi(s \otimes a) = s\psi(a), \quad (s \in [\mathbf{Z}G],\ a \in A). \end{aligned}$$

Since $[\mathbf{Z}G]$ is free as a right H-module, $\bar\varphi$ is again a monomorphism. By the G-injectivity of Q, there exits a G-homomorphism $\bar\zeta : [\mathbf{Z}G] \otimes_{[\mathbf{Z}H]} B \longrightarrow Q$ such that $\bar\zeta\bar\varphi = \bar\psi$. Define $\zeta : B \longrightarrow Q$ by $\zeta(b) = \bar\zeta(1 \otimes b)$. This is easily seen to be the desired H-homomorphism. □

6.7 Special Mappings

In this section we consider some special homomorphisms of (co)homology groups that relate the (co)homology of a group with the (co)homology of its subgroups. We first define special maps and establish results for cohomology groups; in the second part of the section we use duality to obtain corresponding definitions and results for homology. We have already defined the (co)inflation in Section 6.5; it can be regarded as a special map relating the (co)homology of a group and the (co)homology of one of its quotients.

The Restriction Map in Cohomology

Let H be a closed subgroup of a profinite group G. Then every G-module A is automatically an H-module, and the inclusion $H \hookrightarrow G$ is compatible with the identity homomorphism $A \longrightarrow A$. Therefore (see Section 6.5), these maps induced homomorphisms of cohomology groups

$$\mathrm{Res} = \mathrm{Res}^G_H : H^n(G, -) \longrightarrow H^n(H, -) \quad (n \geq 0) \tag{9}$$

that are called *restrictions*.

For each $A \in \mathbf{DMod}(G)$, $A^G \subseteq A^H$. In fact the sequence $\{\mathrm{Res}\}$ is a morphism of cohomological functors $\{H^n(G, -)\}_{n\geq 0} \longrightarrow \{H^n(H, -)\}_{n\geq 0}$; this can be seen from the following equivalent approach to the definition of Res. Since $\{H^n(G,-)\}_{n\geq 0}$ is a universal cohomological functor (see Theorem 6.6.2), the restriction maps (9) are determined by the morphism of functors

$$H^0(G,A) = A^G \hookrightarrow H^0(H,A) = A^H.$$

In terms of cochains these maps can be described as follows. Let $\sigma : G^{n+1} \longrightarrow A$ (continuous) represent an element $\bar{\sigma}$ of $H^n(G,A)$; then a representative n-cocycle $\rho : H^{n+1} \longrightarrow A$ of Res $(\bar{\sigma})$ is given by

$$\rho(x_0,\ldots,x_n) = \sigma(x_0,\ldots,x_n), \quad (x_0,\ldots,x_n \in H).$$

The following proposition is now clear.

Proposition 6.7.1 *Let $G \geq H \geq T$ be profinite groups. Then*

$$\mathrm{Res}_T^H \mathrm{Res}_H^G = \mathrm{Res}_T^G.$$

The Corestriction Map in Cohomology

Let H be an open subgroup of a profinite group G, and let $A \in \mathbf{DMod}(G)$. Since H has finite index, we can define a group homomorphism

$$\mathrm{N}_{G/H} : A^H \longrightarrow A^G$$

by

$$\mathrm{N}_{G/H}(a) = \sum ta,$$

where $a \in A^H$ and t runs through a left transversal of H in G.

Then $\mathrm{N}_{G/H}$ is a well-defined morphism of the functors $H^0(H,-)$ to $H^0(G,-)$ on $\mathbf{DMod}(G)$. By Proposition 6.6.3

$$\{H^n(H,-)\}_{n\geq 0}$$

is a universal cohomological functor $\mathbf{DMod}(G) \longrightarrow \mathfrak{A}$; hence $\mathrm{N}_{G/H}$ extends to a unique morphism of cohomological functors

$$\mathrm{Cor} = \mathrm{Cor}_G^H : \mathbf{H}^\bullet(H,-) \longrightarrow \mathbf{H}^\bullet(G,-).$$

In particular, for every $A \in \mathbf{DMod}(G)$ and every $n \geq 0$, we have a natural homomorphism

$$\mathrm{Cor} = \mathrm{Cor}_G^H : H^n(H,A) \longrightarrow H^n(G,A)$$

which is called the *corestriction* or *transfer*.

Proposition 6.7.2 *Let G be a profinite group and let $T \leq H$ be open subgroups of G. Then*

$$\mathrm{Cor}_G^H \mathrm{Cor}_H^T = \mathrm{Cor}_G^T.$$

Proof. By Lemma 6.1.4 it suffices to verify this result in dimension 0. This in turn follows from the fact that if $\{h_j\}$ is a left transversal of T in H and $\{g_i\}$ a left transversal of H in G, then $\{g_ih_j\}$ is a left transversal of T in G. □

Theorem 6.7.3 *Let H be an open subgroup of a profinite group G. Then the composition* CorRes *is multiplication by the index $[G:H]$ of H in G, i.e.,*

$$\mathrm{Cor}_G^H\mathrm{Res}_H^G = [G:H]\cdot \mathrm{id},$$

where id *is the identity on $H^n(G,-)$ $(n \geq 0)$.*

Proof. Since both $\mathrm{Cor}_G^H\mathrm{Res}_H^G$ and $[G:H]\cdot \mathrm{id}$ are endomorphisms of the cohomological functor $\mathbf{H}^\bullet(G,-)$, it suffices to prove the result on dimension 0 (see Lemma 6.1.4). Let $A \in \mathbf{DMod}(G)$. Then if $a \in A^G$ we have

$$\mathrm{Cor}_G^H\mathrm{Res}_H^G(a) = \mathrm{N}_{G/H}(a) = \sum ta = [G:H]a,$$

as desired. □

Observe that if A is a discrete $[\![\widehat{\mathbf{Z}}G]\!]$-module then $H^n(G,A)$ is torsion (i.e., every element in it has finite order), since its dual $H_n(G,A^*)$ is profinite (see Proposition 6.3.6). The following result extends this to show that $H^n(G,A)$ is torsion for any discrete G-module A (not necessarily torsion).

Corollary 6.7.4 *If G is a profinite group and $A \in \mathbf{DMod}(G)$, then $H^n(G,A)$ is a torsion abelian group for $n \geq 1$. Moreover the order of any element $c \in H^n(G,A)$ divides the order of G.*

Proof. By Corollary 6.5.6 and Proposition 1.2.4, every element of $H^n(G,A)$ is in the image of $H^n(G/U,A^U)$ for some open normal subgroup U of G. Hence, we may assume that G is finite, and prove that in that case $|G|H^n(G,A) = 0$. By Theorem 6.7.3

$$|G|H^n(G,A) = (\mathrm{Cor}_G^1\mathrm{Res}_1^G)(H^n(G,A)) = 0,$$

since obviously $H^n(1,A) = 0$ for $n \geq 1$. □

Corollary 6.7.5 *Let G be a profinite group and let Q be a torsion-free divisible abelian group. Consider Q as a trivial G-module. Then $H^n(G,Q) = 0$ for $n \geq 1$.*

Proof. By Corollary 6.7.4, $H^n(G,Q)$ is a torsion group. Let $0 \neq r \in \mathbf{Z}$. Obviously, multiplication by r is a G-automorphism of Q; hence multiplication by r is an automorphism of $H^n(G,Q)$. The result follows. □

If A is an abelian group and p a prime number, denote by A_p the p-primary component of A (the subgroup consisting of those elements of A whose order is a p-power). By Corollary 6.7.4, $H^n(G,A)$ is a torsion group, and therefore one has

Corollary 6.7.6 *Let G be a profinite group.*

(a) *If $A \in \mathbf{DMod}(G)$, then*

$$H^n(G, A) = \bigoplus_p H^n(G, A)_p.$$

(b) *If $A \in \mathbf{DMod}(\mathbf{Z}G)$, then $H^n(G, A)_p = H^n(G, A_p)$ for every prime p, and consequently,*

$$H^n(G, A) = \bigoplus_p H^n(G, A_p).$$

Corollary 6.7.7 *Let H be a closed subgroup of a profinite group G and let p be a prime number. Assume that $[G : H]$ is not divisible by p. Then the mapping*

$$\mathrm{Res} : H^n(G, A) \longrightarrow H^n(H, A), \quad (n \geq 1)$$

is injective when restricted to $H^n(G, A)_p$. If moreover H is open in G, then the mapping

$$\mathrm{Cor} : H^n(H, A) \longrightarrow H^n(G, A), \quad (n \geq 1)$$

is a surjection of $H^n(H, A)_p$ onto $H^n(G, A)_p$.

Proof. Denote by $\mathcal{V}$ the collection of all open subgroups of G containing H. Then (see Proposition 2.1.4)

$$H = \bigcap_{V \in \mathcal{V}} V = \varprojlim_{V \in \mathcal{V}} V.$$

Therefore, by Proposition 6.5.5,

$$H^n(H, A) = \varinjlim_{V \in \mathcal{V}} H^n(V, A).$$

Notice that the canonical map $H^n(V, A) \longrightarrow H^n(H, A)$ is precisely the restriction map. For each $V \in \mathcal{V}$ we have a commutative diagram (see Proposition 6.7.1).

$$\begin{array}{ccc} H^n(H, A) & \xleftarrow{\mathrm{Res}^{\mathrm{V}}_{\mathrm{H}}} & H^n(V, A) \\ & {\scriptstyle \mathrm{Res}^G_H} \nwarrow \quad \nearrow {\scriptstyle \mathrm{Res}^G_V} & \\ & H^n(G, A)_p & \end{array}$$

Suppose $\mathrm{Res}^G_H(c) = 0$ for some $c \in H^n(G, A)_p$. Then there exists some $V \in \mathcal{V}$ such that $\mathrm{Res}^G_V(c) = 0$ (see Proposition 1.2.4). So, by Theorem 6.7.3,

$$0 = \mathrm{Cor}^V_G \mathrm{Res}^G_V(c) = [G : V]c.$$

Hence $c = 0$, since $([(G : V], p) = 1$. Therefore Res_H^G is injective on $H^n(G, A)_p$.

Assume now that H is open in G. Again by Theorem 6.7.3,

$$\mathrm{Cor}_G^H \mathrm{Res}_H^G : H^n(G, A)_p \longrightarrow H^n(G, A)_p$$

is multiplication by $[G : H]$. However since $p \nmid [G : H]$, multiplication by $[G : H]$ is an automorphism of $H^n(G, A)_p$, and hence

$$\mathrm{Cor}_G^H : H^n(H, A)_p \longrightarrow H^n(G, A)_p$$

is surjective. □

Corollary 6.7.8 *Let G be a profinite group and $A \in$ **DMod**(G). For a prime p, denote by G_p a p-Sylow subgroup of G. If $H^n(G_p, A) = 0$ for every prime p (and a fixed $n \geq 1$), then $H^n(G, A) = 0$.*

Proof. By Corollary 6.7.7, $H^n(G, A)_p = 0$ for each p. Thus

$$H^n(G, A) = \bigoplus_p H^n(G, A)_p = 0. \qquad \square$$

Lemma 6.7.9 *Let G_1 and G_2 be profinite groups and let $\varphi : G_1 \longrightarrow G_2$ be a continuous epimorphism with kernel N. Assume that $K_i \leq_o G_i$ $(i = 1, 2)$ such that $\varphi(K_1) = K_2$. Then, for every $A \in$ **DMod**(G_2) and every natural number n, one has a commutative diagram*

$$\begin{array}{ccc} H^n(K_2, A) & \xrightarrow{[NK_1:K_1]\mathrm{Cor}_{G_2}^{K_2}} & H^n(G_2, A) \\ \downarrow & & \downarrow \\ H^n(K_1, A) & \xrightarrow{\mathrm{Cor}_{G_1}^{K_1}} & H^n(G_1, A) \end{array}$$

where the vertical maps are induced by φ.

Proof. Assume first that $N \leq K_1$. In this case, $[NK_1 : K_1] = 1$ and $[G_1 : K_1] = [G_2 : K_2]$; hence the result follows easily from the definition of corestriction.

Consider next the general case. Form the following diagram

$$\begin{array}{ccccc} H^n(K_2, A) & & \xrightarrow{\qquad [NK_1:K_1]\mathrm{Cor}_{G_2}^{K_2} \qquad} & & H^n(G_2, A) \\ \downarrow & & & & \downarrow \\ H^n(NK_1, A) & \xrightarrow{[NK_1:K_1]\mathrm{id}} & H^n(NK_1, A) & \xrightarrow{\mathrm{Cor}_{G_1}^{NK_1}} & H^n(G_1, A) \\ {\scriptstyle \mathrm{Res}_{K_1}^{NK_1}} \downarrow & & \downarrow {\scriptstyle \mathrm{id}} & & \downarrow {\scriptstyle \mathrm{id}} \\ H^n(K_1, A) & \xrightarrow{\mathrm{Cor}_{NK_1}^{K_1}} & H^n(NK_1, A) & \xrightarrow{\mathrm{Cor}_{G_1}^{NK_1}} & H^n(G_1, A) \end{array}$$

where those maps which are not labeled are induced by φ. Note that $\mathrm{Cor}_{G_1}^{NK_1}\mathrm{Cor}_{NK_1}^{K_1} = \mathrm{Cor}_{G_1}^{K_1}$ (see Proposition 6.7.2), and observe that the composition of the two leftmost vertical maps is just the canonical homomorphism $H^n(K_2, A) \longrightarrow H^n(K_1, A)$ induced by φ. Hence the result will follow if we can prove the commutativity of this diagram. The top rectangle commutes by the case above, since $[G_1 : NK_1] = [G_2 : K_2]$. The lower left rectangle commutes by Theorem 6.7.3. The lower right rectangle is obviously commutative. □

The Corestriction Map in Homology

Let $H \leq G$ be profinite groups and let B be a right profinite $[\![\widehat{\mathbf{Z}}G]\!]$-module. Define the *corestriction* homomorphism of the corresponding homology groups

$$\mathrm{Cor} = \mathrm{Cor}_G^H : H_n(H, B) \longrightarrow H_n(G, B)$$

to be the dual of the restriction homomorphism of the corresponding cohomology groups. Explicitly, when $q = 0$, the corestriction

$$\mathrm{Cor} : H_0(H, B) = B_H \longrightarrow H_0(G, B) = B_G$$

is simply the canonical projection; this is functorial on B, and, in turn, extends to a morphism of universal homological functors

$$\mathrm{Cor} : \{H_n(H, -)\}_{n\geq 0} \longrightarrow \{H_n(G, -)\}_{n\geq 0}.$$

We leave to the reader the description of these mappings in terms of chains.

The Restriction Map in Homology

Assume now that H is an open subgroup of G. The dual of the corestriction maps defined above in cohomology are called the *restriction* homomorphisms

$$\mathrm{Res} = \mathrm{Res}_H^G : H_n(G, B) \longrightarrow H_n(H, B).$$

In dimension zero the restriction homomorphism

$$\mathrm{Res} : H_0(G, B) = B_G \longrightarrow H_0(H, B) = B_H$$

is denoted $N'_{G/H}$ and it is given by

$$N'_{G/H}\big(b + B((IH))\big) = \sum_t bt + B((IG)), \quad (b \in B)$$

with t running through a left transversal of H in G (observe that this map is independent of the chosen transversal, since $th = t + t(h-1)$, and $bt(h-1) \in B_G$, whenever $t \in G$ and $h \in H$). Then $N'_{G/H}$ determines a morphism

$$\text{Res} : \{H_n(G,B)\}_{n\geq 0} \longrightarrow \{H_n(H,B)\}_{n\geq 0}$$

of universal homological functors.

The dual of Theorem 6.7.3 is formally the same for homology:

Theorem 6.7.10 *Let H be an open subgroup of a profinite group G,* CorRes *is multiplication by the index $[G:H]$ of H in G, i.e.,*

$$\text{Cor}_G^H \text{Res}_H^G = [G:S] \cdot \text{id},$$

where id *is the identity on $H_n(G,-)$ $(n \geq 0)$.*

We end this section on special maps by considering the homomorphisms induced by an inner automorphism of a group on the (co)homology groups of its subgroups. We first state the cohomology result.

Proposition 6.7.11 *Let G be a profinite group, H a closed subgroup of G, $A \in \mathbf{DMod}(G)$, and $g \in G$. Let $\iota_g : H \longrightarrow gHg^{-1}$ be the isomorphism given by $\iota_g(x) = gxg^{-1}$, and let $f_g : A \longrightarrow A$ be the group homomorphism defined by $f_g(a) = g^{-1}a$. Then*

(a) *ι_g and f_g are compatible maps and the homomorphisms induced in cohomology*

$$(\iota_g, f_g)^n : H^n(gHg^{-1}, A) \longrightarrow H^n(H,A)$$

are isomorphisms $(n = 0,1,2,\ldots)$.

(b) *If $H \lhd G$ and $g \in H$, the isomorphisms in* (a) *are the identity maps on $H^n(H,A)$ $(n = 0,1,2,\ldots)$.*

(c) *If $H \lhd G$, conjugation in G induces an action of G/H on $H^n(H,A)$ $(n = 0,1,2,\ldots)$.*

Proof. From the definition of $(\iota_g, f_g)^n$ (see Section 6.5), one immediately sees that

$$\{(\iota_g, f_g)^n\}_{n\geq 0} : H^\bullet(gHg^{-1}, -) \longrightarrow H^\bullet(H,-)$$

is a morphism of universal cohomological functors (see Proposition 6.6.3). Hence, by Lemma 6.1.4, it suffices to show that

$$(\iota_g, f_g)^0 : H^0(gHg^{-1}, -) = A^{gHg^{-1}} \longrightarrow H^0(H,-) = A^H$$

is an isomorphism. This map is $a \mapsto g^{-1}a$, which is evidently an isomorphism. This proves (a). For (b), note that if H is normal in G, then $(\iota_g, f_g)^n$ is an endomorphism of $H^n(H,A)$; if moreover $g \in H$, then $(\iota_g, f_g)^0$ is the identity, and hence $(\iota_g, f_g)^n$ is the identity for all $n \geq 0$.

Part (c) is a consequence of (b). □

Dually one has

Proposition 6.7.12 *Let G be a profinite group, H a closed subgroup of G, $B \in \mathbf{PMod}([\![\widehat{\mathbf{Z}}G]\!])$, and $g \in G$. Let $\iota_g : H \longrightarrow gHg^{-1}$ be the isomorphism given by $\iota_g(x) = gxg^{-1}$, and let $f_g : B \longrightarrow B$ be the group homomorphism defined by $f(a) = ag^{-1}$. Then*

(a) *ι_g and f_g are compatible maps and the homomorphisms induced in homology*
$$(\iota_g, f_g)_n : H_n(H, B) \longrightarrow H_n(gHg^{-1}, B)$$
are isomorphisms $(n = 0, 1, 2, \dots)$.
(b) *If $H \triangleleft G$ and $g \in H$, the isomorphisms in* (a) *are the identity maps on $H_n(H, B)$ $(n = 0, 1, 2, \dots)$.*
(c) *If $H \triangleleft G$, conjugation in G induces an action of G/H on $H_n(H, B)$ $(n = 0, 1, 2, \dots)$.*

Remark 6.7.13 See Section 7.2 for an explicit description in terms of cochains of the action of G/H on $H^n(H, A)$ when $H \triangleleft G$.

6.8 Homology and Cohomology Groups in Low Dimensions

In this section we use the definition of (co)homology groups in term of (co)chains to give explicit descriptions of the (co)homology groups $H^0(G, A)$, $H^1(G, A)$, $H^2(G, A)$, $H_0(G, B)$ and $H_1(G, B)$ of a profinite group G.

We have already seen that
$$H^0(G, A) = \{a \in A \mid xa = a, \forall x \in G\} = A^G$$
is the subgroup of elements of A invariant under the action of G.

According to Definition 6.4.1,
$$H^1(G, A) = \mathrm{Ker}(\partial^2)/\mathrm{Im}(\partial^1).$$
The elements of $\mathrm{Ker}(\partial^2)$ are called *crossed homomorphisms* or *derivations* from G to A; so, a crossed homomorphism or derivation
$$d : G \longrightarrow A$$
is a continuous function such that
$$d(xy) = xd(y) + d(x), \quad \text{for all } x, y \in G.$$
We denote the abelian group of derivations by $\mathrm{Der}(G, A)$. The elements of $\mathrm{Im}(\partial^1)$ are called *principal crossed homomorphisms* or *inner derivations*. Each inner derivation $d_a : G \longrightarrow A$ is determined by an element $a \in A$ and is defined by the formula $d_a(x) = xa - a$ $(x \in G)$. The abelian group of all inner derivations from G to A is denoted by $\mathrm{Ider}(G, A)$.

Lemma 6.8.1 *With the notation above we have*

$$H^1(G, A) = \mathrm{Der}(G, A)/\mathrm{Ider}(G, A).$$

Exercise 6.8.2 Let G be a profinite group and A a discrete torsion G-module. Prove that

(a)
$$\mathrm{Der}(G, A) = \varinjlim_{U \in \mathcal{U}} \mathrm{Der}(G/U, A^U),$$

where $\mathcal{U}$ is the collection of all open normal subgroups U of G. (Hint: imitate the proof of Lemma 5.1.4.)

(b) There exists a bijective correspondence between the set of derivations $d : G \longrightarrow A$ and the set of (continuous) group homomorphisms

$$\varphi : G \longrightarrow A \rtimes G$$

such that the composition $G \xrightarrow{f} A \rtimes G \longrightarrow G$ is the identity homomorphism id_G.

The following lemma provides an often useful interpretation of derivations in terms of the augmentation ideal.

Lemma 6.8.3 *Let G be a profinite group and R a commutative profinite ring. Then, for each discrete $[\![RG]\!]$-module A, there is a natural isomorphism*

$$\varphi : \mathrm{Der}(G, A) \longrightarrow \mathrm{Hom}_{[\![RG]\!]}((\!(IG)\!), A)$$

defined by $(\varphi(d))(x-1) = d(x)$, where $(\!(IG)\!) = (\!(I_R G)\!)$ is the augmentation ideal of $[\![RG]\!]$.

Proof. Remark first that

$$\mathrm{Hom}_{[\![RG]\!]}((\!(IG)\!), A) = \varinjlim_{U \in \mathcal{U}} \mathrm{Hom}_{[\![R(G/U)]\!]}((\!(I(G/U))\!), A^U),$$

where $\mathcal{U}$ is the collection of all open normal subgroups U of G (see Lemma 5.1.4). This together with Exercise 6.8.2(a) show that it suffices to prove the result for G finite. By Lemma 6.3.2, $(\!(IG)\!) = (IG)$ is a free R-module on the pointed space $G - 1$. Remark that if $d : G \longrightarrow A$ is a derivation, then $d(1) = 0$; therefore the map

$$\varphi(d) : G - 1 = \{x - 1 \mid x \in G\} \longrightarrow A$$

is a (continuous) mapping of pointed spaces; so, it defines a homomorphism

$$\varphi(d) : I(G) \longrightarrow A$$

of profinite R-modules. Since G is finite, every element of (IG) can be written as a finite sum $\sum_{x\in G}\alpha_x(x-1)$ $(\alpha_x \in R)$. So it is sufficient to show that $\varphi(d)(y(x-1)) = y\varphi(d)(x-1)$. Indeed,

$$\begin{aligned}\varphi(d)(y(x-1)) &= \varphi(d)((yx-1)-(y-1)) = \varphi(d)(yx-1) - \varphi(d)(y-1)\\ &= d(yx) - d(y) = yd(x) = y\varphi(d)(x-1).\end{aligned}$$ □

Next we give an explicit description of the second cohomology group

$$H^2(G, A) = \mathrm{Ker}(\partial^3)/\mathrm{Im}(\partial^2).$$

One readily checks that the elements of $\mathrm{Ker}(\partial^3)$ are precisely those continuous functions $f : G \times G \longrightarrow A$ such that

$$x_1 f(x_2, x_3) - f(x_1x_2, x_3) + f(x_1, x_2x_3) - f(x_1, x_2) = 0 \quad \forall\, x_1, x_2, x_3 \in G.$$

They are called continuous *factor systems*. On the other hand, an element of $\mathrm{Im}(\partial^2)$ is a continuous function $f : G \times G \longrightarrow A$ such that

$$f(x_1, x_2) = x_1 g(x_2) - g(x_1x_2) + g(x_1), \quad (x_1, x_2 \in G)$$

for some continuous $g : G \longrightarrow A$.

$H^2(G, A)$ and Extensions of Profinite Groups

Consider a short exact sequence

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

of profinite groups and continuous homomorphisms, with A finite abelian. Let $\sigma : G \longrightarrow E$ be a continuous section (see Proposition 2.2.2). Define an action $G \times A \longrightarrow A$ of G on A by $(x, a) \mapsto \sigma_x a \sigma_x^{-1}$ $(x \in G,\ a \in A)$. Clearly this action is continuous. This action makes A into a discrete G-module, as one easily verifies. This action is independent of the chosen section because A is abelian.

Given a profinite group G and a finite G-module A, an *extension X of A by G* is defined to be an exact sequence

$$X:\ 0 \longrightarrow A \longrightarrow E \xrightarrow{\varphi} G \longrightarrow 1 \tag{10}$$

with continuous homomorphisms, where E is a profinite group. We shall assume that A and E are written additively (although E is not necessarily abelian), and that the canonical action of G on A described above is precisely the given action of G on A. If X, X' are two extensions of A by G, we say that they are *equivalent* if there exists a continuous homomorphism (necessarily an isomorphism) $E \longrightarrow E'$ such that

$$\begin{array}{ccccccccc} X: & 0 \longrightarrow & A & \longrightarrow & E & \xrightarrow{\varphi} & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \| & & \\ X': & 0 \longrightarrow & A & \longrightarrow & E' & \xrightarrow{\varphi'} & G & \longrightarrow & 1 \end{array}$$

commutes.

Denote by $\mathcal{X}(G, A)$ the set of equivalence classes of extensions of A by G.

Theorem 6.8.4 *Given a profinite group G and a finite G-module A, there exists a one-to-one correspondence between $\mathcal{X}(G, A)$ and $H^2(G, A)$.*

Proof. We only give a sketch; for more details see Ribes [1970]. Consider the extension (10) of A by G, and let $\sigma : G \longrightarrow E$ be a continuous section. Then the action of G on A is given by

$$xa = \sigma(x) + a - \sigma(x), \quad (a \in A,\ \in G).$$

If $x_1, x_2 \in G$, then $\sigma(x_1) + \sigma(x_2)$ and $\sigma(x_1x_2)$ belong to the same coset of A in E. Hence there exists some element $f(x_1, x_2) \in A$ such that

$$\sigma(x_1) + \sigma(x_2) = f(x_1, x_2) + \sigma(x_1x_2).$$

It is clear that $f : G \times G \longrightarrow A$ is a continuous map. One shows easily that it is in fact a continuous factor system.

The definition of f depends on the choice of σ. However, if $\sigma' : G \longrightarrow E$ is another continuous section and $f' : G \times G \longrightarrow A$ its corresponding factor system, define $d(x) \in A$ to be such that

$$\sigma'(x) = d(x) + \sigma(x).$$

Clearly $d : G \longrightarrow A$ is continuous, and one verifies that $f' - f = \partial^2(d)$; therefore f and f' define the same element of $H^2(G, A)$. In fact this last argument shows that if X and X' are equivalent extensions of A by G, they have the same corresponding element in $H^2(G, A)$. Hence we have shown the existence of a well defined map

$$\Phi : \mathcal{X}(G, A) \longrightarrow H^2(G, A).$$

Conversely, let $f : G \times G \longrightarrow A$ be a continuous factor system representing an element of $H^2(G, A)$. We may assume that $f(x, 1) = f(1, x) = 0$, for all $x \in G$. Define a profinite group E in the following manner. The elements of E are the pairs (a, x) $(a \in A,\ x \in G)$. Set

$$(a_1, x_1) + (a_2, x_2) = (a_1 + x_1a_2 + f(x_1, x_2), x_1x_2), \quad (a_1, a_2 \in A,\ x_2, x_2 \in G).$$

With this definition E becomes a group (the associativity follows from f being a factor system) whose zero element is $(0, 1)$, and where

$$-(a,x) = (-x^{-1}a - f(x^{-1},x), x^{-1}).$$

We endow E with the product topology of $A \times G$. Then E is a profinite group, as one easily checks. Moreover

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

(where i and j are the natural injection and projection, respectively), is an extension of A by G. Thus we have defined a map

$$\Psi : H^2(G,A) \longrightarrow \mathcal{X}(G,A).$$

Finally one sees that $\Phi \circ \Psi = \mathrm{id}$ and $\Psi \circ \Phi = \mathrm{id}$. This ends the proof of the theorem. □

Corollary 6.8.5

(a) *The correspondence defined in the theorem above induces an abelian group structure on the set* $\mathcal{X}(G,A)$.
(b) *The extension corresponding to the zero element of* $H^2(G,A)$ *is the split extension, i.e., an extension* (10) *for which there exists a continuous section* $G \longrightarrow E$ *which is a homomorphism. All split extensions are equivalent.*
(c) *Assume that* (10) *is a split extension and let* $\sigma_1, \sigma_2 : G \longrightarrow E$ *be continuous homomorphisms such that* $\varphi\sigma_1 = \mathrm{id}_G = \varphi\sigma_2$. *Define* $d = \sigma_1 - \sigma_2$. *Then* d *is a continuous derivation* $G \longrightarrow A$.

Proof. Parts (a) and (b) are clear. For (c), observe that if $x \in G$, then $\varphi d(x) = \varphi(\sigma_1(x) - \sigma_2(x)) = xx^{-1} = 1$; hence, $d(x) \in A$. In other words, d is a map from G to A. To see that d is a derivation, choose $x, y \in G$; then

$$\begin{aligned} d(xy) &= \sigma_1(xy) - \sigma_2(xy) = \sigma_1(x) + \sigma_1(y) - \sigma_2(y) - \sigma_2(x) \\ &= (\sigma_1(x) + d(y) - \sigma_1(x)) + \sigma_1(x) - \sigma_2(x) = xd(x) + d(y), \end{aligned}$$

as desired. The continuity of d is obvious. □

Now we shall deal with homology in low dimensions. We have already seen that

$$H_0(G,B) = B_G = B/B(\!(IG)\!)$$

(see Lemma 6.3.3). Next we describe $H_1(G,\widehat{\mathbf{Z}})$, $H_1(G,\mathbf{Z}_p)$ and $H_1(G,\mathbf{F}_p)$, where we think of $\widehat{\mathbf{Z}}$, $\mathbf{Z}_p$ and $\mathbf{F}_p$ as a $[\![\widehat{\mathbf{Z}}G]\!]$-modules with trivial G-action.

Lemma 6.8.6

(a) *Let* G *be a profinite group. Then there are isomorphisms*

$$H_1(G,\widehat{\mathbf{Z}}) \cong (\!(IG)\!)/(\!(IG)\!)^2 \cong G/\overline{[G,G]}.$$

These isomorphisms are natural, that is, whenever $\varphi : G \longrightarrow H$ *is a group homomorphism, then the diagram*

$$\begin{array}{ccc} H_1(G,\widehat{\mathbf{Z}}) & \xrightarrow{\cong} & G/\overline{[G,G]} \\ \downarrow & & \downarrow \\ H_1(H,\widehat{\mathbf{Z}}) & \xrightarrow{\cong} & H/\overline{[H,H]} \end{array}$$

commutes, where the vertical maps are induced by φ.

(b) *Let* G *be a pro-*p *group. Then there are natural isomorphisms*

$$H_1(G,\widehat{\mathbf{Z}}_p) \cong [\![IG]\!]/[\![IG]\!]^2 \cong G/\overline{[G,G]}.$$

(c) *Let* G *be a pro-*p *group. Then there is an isomorphism*

$$H_1(G,\mathbf{F}_p) \cong G/\Phi(G).$$

Moreover, this isomorphism is natural in the following sense. If

$$\varphi : G \longrightarrow H$$

is a group homomorphism, then the diagram

$$\begin{array}{ccc} H_1(G,\mathbf{F}_p) & \xrightarrow{\cong} & G/\Phi(G) \\ \downarrow & & \downarrow \\ H_1(H,\mathbf{F}_p) & \xrightarrow{\cong} & H/\Phi(H) \end{array}$$

commutes, where the vertical maps are induced by φ, *and* $\Phi(G)$ *is the Frattini subgroup of* G.

Proof. (a) Put $\Lambda = [\![\widehat{\mathbf{Z}}G]\!]$. Corresponding to the short exact sequence

$$0 \longrightarrow [\![IG]\!] \longrightarrow \Lambda \longrightarrow \widehat{\mathbf{Z}} \longrightarrow 0,$$

there is a long exact sequence in homology (see Proposition 6.3.4)

$$\cdots \to H_1(G,\Lambda) \to H_1(G,\widehat{\mathbf{Z}}) \to H_0(G,[\![IG]\!]) \to H_0(G,\Lambda) \to H_0(G,\widehat{\mathbf{Z}}) \to 0.$$

Since $\Lambda[\![IG]\!] = [\![IG]\!]$, it follows from the above description of $H_0(G,B)$ that

$$H_0(G,[\![IG]\!]) \longrightarrow H_0(G,\Lambda)$$

is the zero map. On the other hand, $H_1(G,\Lambda) = 0$ since Λ is Λ-projective. Therefore, we have an isomorphism

$$H_1(G,\widehat{\mathbf{Z}}) \longrightarrow H_0(G,[\![IG]\!]).$$

By Lemma 6.3.3, $H_0(G, [\![IG]\!]) \cong [\![IG]\!]/[\![IG]\!]^2$. To show the second isomorphism, define a continuous homomorphism

$$\alpha : [\![IG]\!] \longrightarrow G/\overline{[G,G]}$$

of profinite abelian groups by $\alpha(x-1) = x\overline{[G,G]}$; note that this defines in fact a continuous homomorphism for, according to Lemma 6.3.2, $[\![IG]\!]$ is free on the pointed space $\{x-1 \mid x \in G\}$, as a profinite abelian group. Using the formula

$$xy - 1 = (x-1)(y-1) + (x-1) + (y-1), \tag{11}$$

one deduces that $\alpha([\![IG]\!]^2) = 1\overline{[G,G]}$; therefore α induces a homomorphism, that we denote again by the same symbol,

$$\alpha : [\![IG]\!]/[\![IG]\!]^2 \longrightarrow G/\overline{[G,G]}.$$

The map α is in fact an isomorphism. To see this, define a map

$$\beta : G/\overline{[G,G]} \longrightarrow [\![IG]\!]/[\![IG]\!]^2$$

by $\beta(g\overline{[G,G]}) = g - 1 + [\![IG]\!]^2$ $(g \in G)$; it follows again from (11) that β is a well-defined homomorphism. It is plain that α and β are inverse of each other.

The naturality of the second isomorphism follows from the explicit formula used to define it. The naturality of the first isomorphism is a consequence of the commutativity of the diagram

$$\begin{array}{ccc} H_1(G, \widehat{\mathbf{Z}}) & \longrightarrow & H_0(G, [\![IG]\!]) \\ \downarrow & & \downarrow \\ H_1(H, \widehat{\mathbf{Z}}) & \longrightarrow & H_0(H, [\![IH]\!]), \end{array}$$

where the vertical homomorphisms are induced by $\varphi : G \longrightarrow H$.

(b) This is similar to the proof of (a); simply replace $\widehat{\mathbf{Z}}$ by $\mathbf{Z}_p$.

(c) Consider the short exact sequence

$$0 \longrightarrow \mathbf{Z}_p \stackrel{p}{\longrightarrow} \mathbf{Z}_p \longrightarrow \mathbf{F}_p \longrightarrow 0,$$

where the map $\mathbf{Z}_p \stackrel{p}{\longrightarrow} \mathbf{Z}_p$ is multiplication by p. Correspondingly there is a long exact sequence

$$\cdots \to H_1(G, \mathbf{Z}_p) \stackrel{p}{\to} H_1(G, \mathbf{Z}_p) \to H_1(G, \mathbf{F}_p) \to H_0(G, \mathbf{Z}_p) \stackrel{p}{\longrightarrow} H_0(G, \mathbf{Z}_p).$$

Since $H_0(G, \mathbf{Z}_p) \stackrel{p}{\longrightarrow} H_0(G, \mathbf{Z}_p) = \mathbf{Z}_p \stackrel{p}{\longrightarrow} \mathbf{Z}_p$ is a monomorphism, we have that

$$H_1(G, \mathbf{Z}_p) \stackrel{p}{\to} H_1(G, \mathbf{Z}_p) \to H_1(G, \mathbf{F}_p) \to 0$$

is exact. This together with part (b) imply that

$$H_1(G, \mathbf{F}_p) \cong G/G^p\overline{[G,G]}.$$

Clearly this isomorphism is natural. □

6.9 Extensions of Profinite Groups with Abelian Kernel

The purpose of this section is to describe conditions under which certain extensions of profinite groups 'split' i.e., they are semidirect products. One such condition is that the kernel of the extension is a Hall subgroup (see Theorem 2.3.15). In this section we consider only extensions whose kernel is abelian. As in Section 6.8, it is convenient to write such an extension as an exact sequence of profinite groups of the form

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

with A abelian and the map $A \longrightarrow E$ is the inclusion, where A and E are written additively and G multiplicatively. It should be emphasized that E **is not necessarily abelian**.

Let T be a closed subgroup of G and let $\sigma : T \longrightarrow G$ be continuous homomorphism such that $\varphi\sigma = \mathrm{id}_T$. Then we say that σ is a continuous T-*splitting* of the extension $X(A)$. A continuous G-splitting is usually called simply a continuous *splitting* of $X(A)$. If $X(A)$ has a continuous splitting, then one says that $X(A)$ splits (see Corollary 6.8.5).

Since A is abelian, one has that $A = \prod_p A_p$ (see Proposition 2.3.8), where p runs through the prime numbers and A_p is the p-Sylow subgroup of A. For a prime q, denote by $A_{\check{q}}$ the direct product of all A_p such that $p \neq q$. Then $A = A_q \times A_{\check{q}}$, $A_{\check{q}} \triangleleft E$ and $\bigcap_q A_{\check{q}} = 0$.

Lemma 6.9.1 *Consider the extension $X(A)$ above. Then $X(A)$ has a continuous section* (*respectively, splitting*) *if and only if for each prime p, the induced extension*

$$X(A/A_{\check{p}}):\ 0 \longrightarrow A/A_{\check{p}} \longrightarrow E/A_{\check{p}} \xrightarrow{\varphi_p} G \longrightarrow 1$$

has a continuous section (*respectively, splitting*)*.*

Proof. Assume that $\sigma : G \longrightarrow E$ is a continuous section (respectively, splitting) for $X(A)$. Then the composite map $G \xrightarrow{\sigma} E \longrightarrow E/A_{\check{p}}$ is a continuous section (respectively, splitting) for the extension $X(A/A_{\check{p}})$, for every prime p. Conversely, assume that for each p there is a continuous section (respectively, splitting) $\sigma_p : G \longrightarrow E/A_{\check{p}}$ of $X(A/A_{\check{p}})$. Denote by Δ the diagonal subgroup of the direct product $\prod_p G$ of copies of G indexed by the set of prime numbers, i.e., $\Delta = \{(g) \mid g \in G\}$. Consider the following diagram:

$$\begin{array}{ccccc}
\prod_p A/A_{\check{p}} & \longrightarrow & \prod_p E/A_{\check{p}} & \overset{\prod \varphi_p}{\underset{\prod \sigma_p}{\rightleftarrows}} & \prod_p G \\
\psi_{|A} \uparrow \cong & & \psi \uparrow & & \uparrow \rho \\
A & \longrightarrow & E & \xrightarrow[\varphi]{} & G
\end{array}$$

where ψ is the continuous homomorphism that sends e in E to the tuple $(e + A_{\check{p}})$; and where ρ sends G isomorphically to the diagonal subgroup Δ: $g \mapsto (g)$.

Clearly $(\prod \varphi_p)\psi = \rho\varphi$. Since $\bigcap_p A_{\check{p}} = 0$, ψ is a monomorphism; furthermore, we claim that

$$\psi(E) = \left(\prod \varphi_p\right)^{-1}(\Delta).$$

Obviously, $\psi(E) \leq (\prod \varphi_p)^{-1}(\Delta)$. Conversely, assume that $(e_p + A_{\check{p}}) \in (\prod \varphi_p)^{-1}(\Delta)$, where $e_p \in E$ for all p; then, there exists some $g \in G$ such that $\varphi(e_p) = g$ for all p. Choose $e \in E$ such that $\varphi(e) = g$. Then $(\prod \varphi_p)(e_p - e + A_{\check{p}}) = 1$. Hence $(e_p - e + A_{\check{p}}) \in \prod_p A/A_{\check{p}}$. Since

$$\psi_{|A} : A \longrightarrow \prod_p A/A_{\check{p}}$$

is an isomorphism, there exists $a \in A$ with $\psi(a) = (e_p - e + A_{\check{p}})$. Therefore, $\psi(a + e) = (e_p + A_{\check{p}})$. Thus, $\psi(E) \geq (\prod \varphi_p)^{-1}(\Delta)$, proving the claim.

Hence, the image of the continuous map (respectively, homomorphism)

$$\left(\prod \sigma_p\right)\rho : G \longrightarrow \prod_p E/A_{\check{p}}$$

is contained in $\psi(E)$. Thus $\psi^{-1}(\prod \sigma_p)\rho : G \longrightarrow E$ is a continuous section (respectively, splitting) for the extension $X(A)$. □

Theorem 6.9.2 *Assume that for every prime number p, the extension $X(A)$ above has a continuous G_p-splitting, where G_p is some p-Sylow subgroup of G. Then the extension $X(A)$ splits.*

By Lemma 6.9.1, it suffices to consider the following special case.

Theorem 6.9.3 *Let p be a fixed prime number. Assume that A is an abelian pro-p group and assume that the extension $X(A)$ has a continuous G_p-splitting, where G_p is some p-Sylow subgroup of G. Then the extension $X(A)$ splits.*

Proof. We shall prove this theorem in several steps. The idea of the proof for general A is to consider appropriate short exact sequences obtained by taking finite quotients of A and then use an inverse limit argument. The main difficulty is that for finite A, the number of splittings of $X(A)$ is not necessarily finite; the key of the proof is to exhibit the existence of a canonical finite set of splittings in that case.

Step 1. Assume that A is a finite abelian p group. We show that in this case, $X(A)$ splits.

According to Theorem 6.8.4 and Corollary 6.8.5, the extension $X(A)$ corresponds canonically to an element $\bar{f} \in H^2(G, A)$, where $f : G \times G \longrightarrow A$ is a 2-cocycle (a continuous factor system); moreover, $X(A)$ splits if and only if $\bar{f}=0$. By our assumptions, $\mathrm{Res}^G_{G_p}(\bar{f})=0$. By Corollary 6.7.7, $\mathrm{Res}^G_{G_p}$ is a monomorphism; therefore $\bar{f}=0$.

Step 2. Assume that A is a finite abelian p group. We identify $H^n(G,A)$ with its image $\mathrm{Res}^G_{G_p}(H^n(G,A))$ in $H^n(G_p,A)$ (this is permissible since in this case $\mathrm{Res}^G_{G_p}$ is a monomorphism by Corollary 6.7.7). We show that there exists a canonical decomposition

$$H^n(G_p,A)=H^n(G,A)\oplus K \quad (n\geq 1),$$

where K is described below (of course, K depends on n).

First we assert that if G is finite, then $H^n(G_p,A)=H^n(G,A)\oplus K$, where $K=\mathrm{Ker}(\mathrm{Cor}^{G_p}_G)$. Indeed, when G is finite,

$$\mathrm{Cor}^{G_p}_G\mathrm{Res}^G_{G_p}: H^n(G,A)\longrightarrow H^n(G,A)$$

is multiplication by $[G:G_p]$; since $H^n(G,A)$ is finite and p-primary, multiplication by $[G:G_p]$ is an isomorphism. Thus the assertion easily follows.

If G is infinite, let $\mathcal{U}$ be the collection of all open normal subgroups of E such that $U\cap A=1$; put $\tilde{U}=\varphi(U)$. For each $U\in\mathcal{U}$, there is a corresponding extension

$$0\longrightarrow A\longrightarrow E/U\longrightarrow G/\tilde{U}\longrightarrow 1.$$

By the above assertion, there is a canonical decomposition

$$H^n(\tilde{U}G_p/\tilde{U},A)=H^n(G/\tilde{U},A)\oplus K(U),$$

where $K(U)$ is the kernel of $\mathrm{Cor}^{\tilde{U}G_p/U}_{G/\tilde{U}}: H^n(\tilde{U}G_p/\tilde{U},A)\longrightarrow H^n(G/\tilde{U},A)$. Let $U,V\in\mathcal{U}$ be such that $V\leq U$. Denote by $\rho: E/V\longrightarrow E/U$ the natural epimorphism. Then ρ induces a homomorphism

$$H^n(\rho,A): H^n(\tilde{U}G_p/\tilde{U},A)\longrightarrow H^n(\tilde{V}G_p/\tilde{V},A).$$

Clearly $H^n(\rho,A)$ sends $H^n(G/\tilde{U},A)$ to $H^n(G/\tilde{V},A)$, since $H^n(\rho,A)$ commutes with Res. Moreover, $H^n(\rho,A)$ sends $K(U)$ to $K(V)$, by Lemma 6.7.9: let the pairs $(G/\tilde{V},\tilde{V}G_p/\tilde{V})$ and $(G/\tilde{U},\tilde{U}G_p/\tilde{U})$ play the role of (G_1,K_1) and (G_2,K_2), respectively.

Therefore, taking direct limits, one has (see Corollary 6.5.6)

$$\begin{aligned} H^n(G_p,A) &= \varinjlim_{U\in\mathcal{U}} H^n(\tilde{U}G_p/\tilde{U},A)\\ &= \varinjlim_{U\in\mathcal{U}} H^n(G/\tilde{U},A)\oplus \varinjlim_{U\in\mathcal{U}} K(U)=H^n(G,A)\oplus K, \end{aligned}$$

since the functor $\varinjlim$ is exact in the category of abelian groups (see Proposition 1.2.6).

Step 3. Assume still that A is a finite abelian p group. We shall prove the existence of a canonical nonempty finite set $\mathcal{S}$ of continuous splittings of $X(A)$.

First we define the concept of 'closeness' of two continuous G_p-splittings $\sigma, \sigma' : G_p \longrightarrow E$ of $X(A)$. Put $z(\sigma, \sigma') = \sigma' - \sigma$. Then $z(\sigma, \sigma')$ is a continuous derivation, $z(\sigma, \sigma') = \sigma' - \sigma : G_p \longrightarrow A$ (see Corollary 6.8.5). Denote by $\tilde{z}(\sigma, \sigma')$ the corresponding class in $H^1(G_p, A)$. We say that σ and σ' are *close* if, in the canonical decomposition of Step 2 (for $n = 1$)

$$H^1(G_p, A) = H^1(G_p, A_p) = H^1(G, A) \oplus K, \tag{12}$$

one has that $\tilde{z}(\sigma, \sigma') \in K$.

By hypothesis, there exists a certain G_p-splitting of $X(A)$, $\gamma : G_p \longrightarrow E$, that we fix. Define $\mathcal{S}$ to consist of those G-splittings Γ of $X(A)$ such that Γ_p and γ are close, where Γ_p denotes the restriction of Γ to G_p.

We make two claims.

Claim 1: $\mathcal{S} \neq \emptyset$, and

Claim 2: $\mathcal{S}$ is a finite set (more precisely, two elements of $\mathcal{S}$ are conjugate by an element of A).

By Step 1, the extension $X(A)$ admits a continuous G-splitting $\Gamma' : G \longrightarrow E$. Denote by Γ'_p its restriction to G_p. Use (12) to find a decomposition

$$\tilde{z}(\Gamma'_p, \gamma) = \tilde{u} + k,$$

where $k \in K$ and $\tilde{u} \in H^1(G, A_p)$. Choose a continuous derivation $u : G \longrightarrow A$ in $\tilde{u}$. Put $\Gamma = u + \Gamma'$. Then Γ is a continuous G-splitting of $X(A)$ and clearly Γ_p and γ are close. This proves Claim 1.

To prove Claim 2, let $\Gamma, \Gamma' \in \mathcal{S}$ and let $u = \Gamma - \Gamma'$. Then $u : G \longrightarrow A$ is a continuous derivation. Note that

$$\mathrm{Res}^G_{G_p}(\tilde{u}) = \tilde{z}(\Gamma_p, \Gamma'_p) \in H^1(G_p, A).$$

Since $\tilde{z}(\Gamma_p, \gamma), \tilde{z}(\Gamma'_p, \gamma) \in K$, we have that $\tilde{z}(\Gamma_p, \Gamma'_p) \in K$. On the other hand, since we have identified $H^1(G, A)$ with its image in $H^1(G_p, A)$ under the map $\mathrm{Res}^G_{G_p}$, we have that $\tilde{u} = \tilde{z}(\Gamma_p, \Gamma'_p) \in H^1(G, A)$. Therefore, $\tilde{u} \in H^1(G, A) \cap K = 0$. Thus, u is an inner derivation; hence, there exists some $a \in A$ such that $u(g) = ga - a$, for every $g \in G$. Since A is finite, there are only finitely many possibilities for $u = \Gamma - \Gamma'$. Hence, the set $\mathcal{S}$ is finite. (Note that for $g \in G$, one has $u(g) = \Gamma(g) - \Gamma'(g) = ga - a = \Gamma(g) + a - \Gamma(g) - a$; hence $\Gamma'(g) = a + \Gamma(g) - a$; i.e., Γ' is the a-conjugate of Γ.)

Step 4. General case: A is any abelian pro-p group.

Let $\mathcal{V} = \{V \triangleleft_o A \mid V = A \cap U \text{ for some } U \triangleleft_o E\}$. For each $V \in \mathcal{V}$, consider the extension of profinite groups

$$X(A/V) : \ 0 \longrightarrow A/V \longrightarrow E/V \xrightarrow{\varphi_V} G \longrightarrow 1,$$

where φ_V is induced by φ. If $V, V' \in \mathcal{V}$ with $V \leq V'$, denote by

$$\epsilon(V, V') : X(A/V) \longrightarrow X(A/V')$$

the map of extensions naturally induced by $E/V \longrightarrow E/V'$. The extensions $X(A/V)$ together with the maps $\epsilon(V, V')$ $(V, V' \in \mathcal{V})$ form an inverse system, and clearly

$$\varprojlim_{V \in \mathcal{V}} X(A/V) = X(A).$$

Denote by $\mathcal{S}_V$ the canonical finite set of continuous G-splittings described in Case 3 for the extension $X(A/V)$. Let $V, V' \in \mathcal{V}$ with $V \leq V'$, and assume that $\Gamma : G \longrightarrow E/V$ is a G-splitting of $X(A/V)$ contained in $\mathcal{S}_V$. Then by the construction of the sets $\mathcal{S}_V$, the map $G \xrightarrow{\Gamma} G/V \longrightarrow G/V'$ is a G-splitting of $X(A/V')$ contained in $\mathcal{S}_{V'}$. In other words, $\epsilon(V, V')$ induces a map $\mathcal{S}_V \longrightarrow \mathcal{S}_{V'}$. Hence, the sets $\mathcal{S}_V$ $(V \in \mathcal{V})$ together with these maps form an inverse system of nonempty finite sets. Thus (see Proposition 1.1.4),

$$\varprojlim_{V \in \mathcal{V}} \mathcal{S}_V \neq \emptyset.$$

Let

$$(\Gamma_V)_{V \in \mathcal{V}} \in \varprojlim_{V \in \mathcal{V}} \mathcal{S}_V.$$

Define

$$\Gamma = \varprojlim_{V \in \mathcal{V}} \Gamma_V.$$

Then $\Gamma : G \longrightarrow E$ is a continuous splitting of the extension $X(A)$. □

6.10 Induced and Coinduced Modules

Let G be a profinite group and let $H \leq_c G$. For $A \in \mathbf{DMod}(H)$ consider the abelian group

$$\operatorname{Coind}_H^G(A) = \{f : G \longrightarrow A \mid f \text{ continuous}, \\ \text{with } f(hy) = hf(y) \text{ for all } h \in H,\ y \in G\}.$$

The compact-open topology makes $\operatorname{Coind}_H^G(A)$ into a discrete abelian group. Define an action of G on $\operatorname{Coind}_H^G(A)$ by

$$(xf)(y) = f(yx) \quad (x, y \in G,\ f \in \operatorname{Coind}_H^G(A)).$$

This action is in fact continuous. To see this we must show that the G-stabilizer of each element of $\operatorname{Coind}_H^G(A)$ is open in G, according to Lemma 5.3.1. Indeed, assume $f \in \operatorname{Coind}_H^G(A)$ and let $G_f = \{x \in G \mid xf = f\}$ be its stabilizer. For each $x \in G$, choose an open normal subgroup U_x of G

such that $xU_x \subseteq f^{-1}(f(x))$. By compactness there exist finitely many points $x_1, \dots, x_n$ such that

$$G = \bigcup_{i=1}^{n} x_i U_{x_i}.$$

Put $U = \bigcap_{i=1}^{n} U_{x_i}$. We claim that $xU \subseteq f^{-1}(f(x))$, for each $x \in G$. To see this consider $x \in G$; then $x = x_i u_i$ for some $i = 1, \dots, n$ and some $u_i \in U_i$. Hence, $f(x) = f(x_i)$. Now, if $u \in U$, then $xu = x_i u_i u \in x_i U_i$. Thus $f(xu) = f(x_i) = f(x)$. This proves the claim. Therefore, $(uf)(x) = f(xu) = f(x)$, whenever $x \in G$, $u \in U$. Hence $U \subseteq G_f$, showing that G_f is open, as asserted.

The G-module $\mathrm{Coind}_H^G(A)$ is called a *coinduced* module.* It is easy to see that $\mathrm{Coind}_H^G(-)$ is an additive functor from $\mathbf{DMod}(H)$ into $\mathbf{DMod}(G)$.

Remark 6.10.1 If the discrete G-module A is torsion, then in fact A is a discrete $[\![\widehat{\mathbf{Z}}G]\!]$-module (see Proposition 5.3.6(e)). In this case one clearly has $\mathrm{Coind}_H^G(A) = \mathrm{Hom}_{[\![\widehat{\mathbf{Z}}H]\!]}([\![\widehat{\mathbf{Z}}G]\!], A)$. In particular, if H is the trivial group, then $\mathrm{Coind}_1^G(A) = \mathrm{Hom}_{\widehat{\mathbf{Z}}}([\![\widehat{\mathbf{Z}}G]\!], A)$.

The following is an analogue of Proposition 5.5.4(c) for non-necessarily torsion A.

Lemma 6.10.2 *Let G be a profinite group, H a closed subgroup of G, A a discrete H-module and A' a discrete G-module. Then there exists a natural isomorphism*

$$\mathrm{Hom}_G(A', \mathrm{Coind}_H^G(A)) \cong \mathrm{Hom}_H(A', A).$$

Proof. Given $\varphi \in \mathrm{Hom}_G(A', \mathrm{Coind}_H^G(A))$, define $\bar{\varphi} : A' \longrightarrow A$ by $\bar{\varphi}(a') = \varphi_{a'}(1)$ $(a' \in A')$; then $\bar{\varphi} \in \mathrm{Hom}_H(A', A)$. Conversely, if $\psi \in \mathrm{Hom}_H(A', A)$, define $\tilde{\psi} : A' \longrightarrow \mathrm{Coind}_G^H(A)$ by $\tilde{\psi}_{a'}(x) = \psi(xa')$ $(a' \in A',\ x \in G)$; then indeed $\tilde{\psi}_{a'} \in \mathrm{Coind}_G^H(A)$ and $\tilde{\psi} \in \mathrm{Hom}_G(A', \mathrm{Coind}_G^S(A))$. One easily verifies that the maps $\varphi \mapsto \bar{\varphi}$ and $\psi \mapsto \tilde{\psi}$ are homomorphisms and inverse to each other; hence the result. □

Corollary 6.10.3 *The functor* $\mathrm{Coind}_H^G(-)$ *sends injective H-modules to injective G-modules.*

Proof. Let Q be an injective H-module. Then, by definition of injectivity, the functor $\mathrm{Hom}_H(-, Q) : \mathbf{DMod}(H) \longrightarrow \mathfrak{A}$ is exact ($\mathfrak{A}$ is the category of abelian groups). The isomorphism in Lemma 6.10.2 implies that the functor $\mathrm{Hom}_G(-, \mathrm{Coind}_H^G(Q)) : \mathbf{DMod}(G) \longrightarrow \mathfrak{A}$ is also exact; hence $\mathrm{Coind}_H^G(Q)$ is G-injective. □

---

* Note that these modules are called 'induced' in Serre [1995], Ribes [1970] and Shatz [1972], where they are denoted by $M_G^H(A)$. In this book we adopt a terminology and notation which is more in accordance to the traditional use of the term 'coinduced' in the context of the cohomology of abstract groups.

Proposition 6.10.4 *Let G be a profinite group, H a closed subgroup of G and A a discrete H-module. Then*

(a)

$$\operatorname{Coind}_H^G(A) = \varinjlim_{U \in \mathcal{U}} \operatorname{Coind}_{HU/U}^{G/U}(A^{U\cap H}),$$

where $\mathcal{U}$ is the collection of open normal subgroups of G.
(b) $\operatorname{Coind}_H^G(-)$ *is an exact functor.*

Proof. The proof of (a) is similar to the proof of Lemma 5.1.4(a) and we leave it to the reader. Using (a), in the proof of (b) we may assume that G is finite, since $\varinjlim$ is an exact functor. In this case, note that

$$\operatorname{Coind}_H^G(-) = \operatorname{Hom}_{[\mathbf{Z}H]}([\mathbf{Z}G], -).$$

Now, $[\mathbf{Z}G]$ is a direct sum of $|G/H|$ copies of $[\mathbf{Z}H]$; hence $[\mathbf{Z}G]$ is $[\mathbf{Z}H]$-projective; thus $\operatorname{Hom}_{[\mathbf{Z}H]}([\mathbf{Z}G], -)$ is exact. □

Let $H \leq_c G$ be profinite groups and $A \in \mathbf{DMod}(H)$. Then there exists a canonical H-homomorphism

$$\mu : \operatorname{Coind}_H^G(A) \longrightarrow A$$

given by

$$\mu(f) = f(1), \quad \text{for all } f \in \operatorname{Coind}_H^G(A). \tag{13}$$

Theorem 6.10.5 (Shapiro's Lemma) *Let G be a profinite group, H a closed subgroup of G and $A \in \mathbf{DMod}(H)$. Then there exist natural isomorphisms*

$$H^n(G, \operatorname{Coind}_H^G(A)) \cong H^n(H, A) \quad (n \geq 0).$$

Proof. By Corollary 6.10.3, Proposition 6.10.4 and Theorem 6.6.2

$$H^\bullet(H, -) \quad \text{and} \quad H^\bullet(G, \operatorname{Coind}_H^G(-))$$

are effaceable cohomological functors on the category $\mathbf{DMod}(H)$. We shall show that the morphism of cohomological functors

$$H^n(G, \operatorname{Coind}_H^G(A)) \xrightarrow{\text{Res}} H^n(H, \operatorname{Coind}_H^G(A)) \xrightarrow{\bar\mu} H^n(H, A)$$

is an isomorphism, where $\bar\mu$ is induced by μ (see (13)). It suffices to do this in dimension zero.

For $n = 0$ this map is the following: the element $f \in (\operatorname{Coind}_H^G(A))^G = H^0(G, \operatorname{Coind}_H^G(A))$ is mapped to $f(1)$ (note that $f(x) = f(1)$, for all $x \in G$; hence for $h \in H$, one has that $hf(1) = f(h) = f(1)$; and so $f(1) \in A^H$). To see that this is an isomorphism, check that the following is its inverse: if $a \in A^H$, put $f : G \longrightarrow A$ to be the constant function $f(x) = a$, for all $x \in G$; then $f \in (\operatorname{Coind}_H^G(A))^G = H^0(G, \operatorname{Coind}_H^G(A))$. □

Corollary 6.10.6 *Let G be a profinite group and let A be an abelian group. Then* $\mathrm{Coind}_1^G(A) = C(G, A)$ *(the group of all continuous functions from G to A), and* $H^n(G, C(G, A)) = 0$ *for $n > 0$.*

Proof. The first assertion is clear. For the second we use the theorem above, $H^n(G, C(G, A)) = H^n(G, \mathrm{Coind}_1^G(A)) \cong H^n(1, A) = 0$ $(n > 0)$. □

The dual concept of a coinduced module is that of an induced module. Let $H \le G$ be profinite groups and let B be a profinite right $[\![\widehat{\mathbf{Z}}H]\!]$-module. Define a right G-module structure on the profinite group

$$\mathrm{Ind}_H^G(B) = B \,\widehat{\otimes}_{[\![\widehat{\mathbf{Z}}H]\!]}\, [\![\widehat{\mathbf{Z}}G]\!]$$

by $(b\widehat{\otimes}r)g = b\widehat{\otimes}rg$ ($g \in G$, $b \in B$, $r \in [\![\widehat{\mathbf{Z}}G]\!]$). Then $\mathrm{Ind}_H^G(B)$ is called an *induced* $[\![\widehat{\mathbf{Z}}G]\!]$-module.

Using Proposition 5.5.4(c) one obtains immediately the following result.

Lemma 6.10.7 *Let $H \le G$ be profinite groups and let B be a profinite right $[\![\widehat{\mathbf{Z}}H]\!]$-module. Then* $\mathrm{Ind}_H^G(B)$ *and* $\mathrm{Coind}_H^G(B^*)$ *are Pontryagin dual.*

Hence, by duality one obtains automatically the following results from Corollary 6.10.3, Proposition 6.10.4, Theorem 6.10.5 and Corollary 6.10.6 (remark that part (c) of the following theorem can be also deduced from the fact that $[\![\widehat{\mathbf{Z}}G]\!]$ is $[\![\widehat{\mathbf{Z}}H]\!]$-projective; however Proposition 6.10.4 cannot be obtained in full generality from this using duality, since the module A may not be torsion).

Theorem 6.10.8 *Let G be a profinite group, H a closed subgroup of G and* $B \in \mathbf{PMod}([\![\widehat{\mathbf{Z}}H]\!])$.

(a) *The functor* $\mathrm{Ind}_H^G(-)$ *sends projective profinite $[\![\widehat{\mathbf{Z}}H]\!]$-modules to projective profinite $[\![\widehat{\mathbf{Z}}G]\!]$-modules.*

(b)
$$\mathrm{Ind}_H^G(B) = \varprojlim_{U \in \mathcal{U}} \mathrm{Ind}_{HU/U}^{G/U}(B_{U\cap H}),$$

where $\mathcal{U}$ is the collection of open normal subgroups of G.

(c) $\mathrm{Ind}_H^G(-)$ *is an exact functor.*

(d) (Shapiro's Lemma) *There exist natural isomorphisms*

$$H_n(G, \mathrm{Ind}_H^G(B)) \cong H_n(H, B), \quad (n \ge 0).$$

(e) *Let M be a profinite abelian group. Then* $\mathrm{Ind}_1^G(M) = M\widehat{\otimes}_{\widehat{\mathbf{Z}}}[\![\widehat{\mathbf{Z}}G]\!]$, *and*

$$H_n(G, M \,\widehat{\otimes}_{\widehat{\mathbf{Z}}}\, [\![\widehat{\mathbf{Z}}G]\!]) = 0$$

for $n > 0$.

It is easy to give a direct proof of Shapiro's Lemma for homology (but we remark that this is not good enough for cohomology since in that case we want the proof to be valid for all discrete G-modules, even if they are not torsion). We do this in the next lemma for a general commutative profinite ring R.

Theorem 6.10.9 (Shapiro's Lemma) *Let G be a profinite group, H a closed subgroup of G, R a commutative profinite ring and $B \in \mathbf{PMod}([\![RH]\!])$. Then, there are natural isomorphisms*

$$H_n(G, B \,\widehat{\otimes}_{[\![RH]\!]}\, [\![RG]\!]) \cong H_n(H, B) \quad (n \geq 0).$$

Proof. Since $[\![RG]\!]$ is a free $[\![RH]\!]$-module, the functor $- \,\widehat{\otimes}_{[\![RH]\!]}\, [\![RG]\!]$ is exact; hence $\{H_n(G, - \,\widehat{\otimes}_{[\![RH]\!]}\, [\![RG]\!]\}_{n\in\mathbf{N}}$ is a universal homological sequence of functors from $\mathbf{PMod}([\![RH]\!])$ to $\mathbf{PMod}(R)$. By Proposition 6.6.3, this is also the case for the sequence $\{H_n(H, -)\}_{n\in\mathbf{N}}$. Hence, it suffices to prove the lemma in dimension 0. But this case is clear:

$$H_0(G, B \,\widehat{\otimes}_{[\![RH]\!]}\, [\![RG]\!]) = B \,\widehat{\otimes}_{[\![RH]\!]}\, [\![RG]\!] \,\widehat{\otimes}_{[\![RG]\!]}\, R \cong B \,\widehat{\otimes}_{[\![RH]\!]}\, R = H_0(H, B).$$

□

Next we observe that if A and B are $[\![RG]\!]$-modules, then

$$B \,\widehat{\otimes}_{[\![RG]\!]}\, A = (B \,\widehat{\otimes}_R\, A)_G,$$

where G acts on $(B \,\widehat{\otimes}_R\, A)_G$ diagonally. This is clear for abstract tensor products (it follows from the definition), and for complete tensor products it follows by taking inverse limits.

We record next a technical result for future reference.

Lemma 6.10.10 *Let G be a profinite group, H a closed subgroup of G and R a commutative profinite ring. Let B be a right $\mathbf{PMod}([\![RG]\!])$-module. Then*

(a) *For each $n = 0, 1, \ldots$ there exist natural isomorphisms*

$$\varphi_n : \mathrm{Tor}_n^{[\![RG]\!]}(B, [\![R(G/H)]\!]) \longrightarrow H_n(H, B).$$

(b) *For each n, there is a commutative diagram*

$$\begin{array}{ccc} \mathrm{Tor}_n^{[\![RG]\!]}(B, [\![R(G/H)]\!]) & \xrightarrow{\varepsilon_n} & H_n(G, B) \\ \downarrow{\scriptstyle \varphi_n} & \nearrow{\scriptstyle \mathrm{Cor}} & \\ H_n(H, B) & & \end{array}$$

where ε_n is the map induced by the augmentation map $[\![R(G/H)]\!] \xrightarrow{\varepsilon} R$.

Proof. (a) Since $\{H_\bullet(H,-)\}_{n\in\mathbf{N}}$ and $\{\mathrm{Tor}_\bullet^{[\![RG]\!]}(-,[\![R(G/H)]\!])\}_{n\in\mathbf{N}}$ are universal homological functors on the category $\mathbf{PMod}([\![RG]\!])$, it suffices to prove the existence of this natural isomorphism in dimension 0. Using the above observation and Proposition 5.8.1, we have

$$\begin{aligned}
&\mathrm{Tor}_0^{[\![RG]\!]}(B,[\![R(G/H)]\!])\\
&\quad= B\,\widehat{\otimes}_{[\![RG]\!]}\,[\![R(G/H)]\!] \cong (B\,\widehat{\otimes}_R[\![R(G/H)]\!])_G\\
&\quad\cong ((B\,\widehat{\otimes}_R[\![R(G/H)]\!])\,\widehat{\otimes}_R R)_G \cong (B\,\widehat{\otimes}_R[\![R(G/H)]\!])\,\widehat{\otimes}_{[\![RG]\!]}\,R\\
&\quad\cong (B\,\widehat{\otimes}_{[\![RH]\!]}\,[\![RG]\!])\,\widehat{\otimes}_{[\![RG]\!]}\,R \cong B\,\widehat{\otimes}_{[\![RH]\!]}\,R = H_0(H,B),
\end{aligned}$$

as needed.

For use in part (b), we remark that if $b\in B$ and $s\in[\![R(G/H)]\!]$, then $\varphi_0(b\,\widehat{\otimes}\,s) = b\,\widehat{\otimes}\,\varepsilon(s)$. To see this it is enough to check it when $s = r(Hg)$ $r\in R, g\in G$); in this case one easily verifies the assertion with the explicit formulas used in the proof of Proposition 5.8.1.

(b) Since

$$\{\mathrm{Tor}_n^{[\![RG]\!]}(-,[\![R(G/H)]\!])\}_{n\in\mathbf{N}},\qquad \{H_n(H,-)\}_{n\in\mathbf{N}}\quad\text{and}\quad\{H_n(G,-)\}_{n\in\mathbf{N}}$$

are universal homological functors from $\mathbf{PMod}([\![RG]\!])$ to $\mathbf{PMod}(R)$, it suffices to prove the commutativity of the diagram in dimension zero. This follows from the remark at the end of part (a), since

$$(\mathrm{Cor}\,\varphi_0)(b\,\widehat{\otimes}\,s) = \mathrm{Cor}(b\,\widehat{\otimes}\,\varepsilon(s)) = b\,\widehat{\otimes}\,\varepsilon(s) = \varepsilon_0(b\,\widehat{\otimes}\,s)$$

for $b\in B, s\in[\![R(G/H)]\!]$. □

6.11 The Induced Module $\mathrm{Ind}_H^G(B)$ for H Open

Let H be an open subgroup of a profinite group G and let R be a commutative profinite ring. Consider a profinite right $[\![RH]\!]$-module B. Next we wish to study $\mathrm{Ind}_H^G(B) = B\,\widehat{\otimes}_{[\![RH]\!]}\,[\![RG]\!]$ in more detail in this special case. Choose a right transversal $\{t \mid t\in T\}$ of H in G with $1\in T$. Then there is a decomposition of left $[\![RH]\!]$-modules

$$[\![RG]\!] \cong \bigoplus_{t\in T}[\![RH]\!]t.$$

Correspondingly, there is a decomposition of R-modules

$$B \cong \bigoplus_{t\in T} B\,\widehat{\otimes}_{[\![RH]\!]}\,[\![RH]\!]t \cong \bigoplus_{t\in T} B\,\widehat{\otimes}\,t,$$

where $B\,\widehat{\otimes}\,t = \{b\,\widehat{\otimes}\,t \mid b\in B\}$. Remark that $B\,\widehat{\otimes}\,t \cong Bt$, as R-modules, so that

$$B \otimes_{[\![RH]\!]} [\![RG]\!] \cong \bigoplus_{t \in T} Bt. \tag{14}$$

In fact this is an isomorphism of $[\![RG]\!]$-modules if one lets G act on $\bigoplus_{t\in T} Bt$ by permuting the summands Bt. More explicitly, for $g \in G$ and $t \in T$, one has

$$tg = h_t(g)t^{\pi_g},$$

where $h_t(g) \in H$ and π_g is the permutation on T induced by the natural continuous action of G on the set $H\backslash G$ of right cosets; then

$$(m \widehat{\otimes} t)g = mh_t(g) \widehat{\otimes} t^{\pi_g}.$$

Observe that the stabilizer of t under the action of G on T is $t^{-1}Ht$, and that Bt is naturally a $t^{-1}Ht$-module. The R-isomorphism $\varphi_t : B \longrightarrow Bt$ given by $m \mapsto mt$, and the isomorphism of groups $\iota_t : H \longrightarrow t^{-1}Ht$ given by $h \mapsto t^{-1}ht$, are compatible, i.e., $\varphi_t(mh) = \varphi_t(m)h^{\iota_t}$. Hence φ_t induces an isomorphism of $[\![RG]\!]$-modules

$$\mathrm{Ind}_H^G(B) = B \widehat{\otimes}_{[\![RH]\!]} [\![RG]\!] \longrightarrow \mathrm{Ind}_{t^{-1}Ht}^G(Bt) = Bt \widehat{\otimes}_{[\![R(t^{-1}Ht)]\!]} [\![RG]\!]$$

given by $m \widehat{\otimes} g \mapsto mt \widehat{\otimes} t^{-1}g$. Then one has the following characterization of induced modules.

Proposition 6.11.1 *Let G be a profinite group and let M be a right $[\![RG]\!]$-module. Suppose that $M = \bigoplus_{i\in I} B_i$ is a direct sum decomposition of M as an R-module, where the indexing set I is finite. Moreover assume that G acts continuously and transitively on the finite set I in such a way that $B_i g = B_{ig}$. Fix $i \in I$ and let H be the stabilizer of i under the action of G. Then $B = B_i$ is a right $[\![RH]\!]$-module and*

$$M \cong \mathrm{Ind}_H^G(B) = B \widehat{\otimes}_{[\![RH]\!]} [\![RG]\!],$$

as $[\![RG]\!]$-modules.

Proof. That B is a right H-module is clear. Note $[G : H] = |I|$. Define

$$\rho : B \widehat{\otimes}_{[\![RH]\!]} [\![RG]\!] \longrightarrow M$$

by $\rho(m \widehat{\otimes} g) = mg \quad (mg \in B_{ig} \subseteq M)$. Then ρ is well-defined and it is an $[\![RG]\!]$-homomorphism. Clearly $B = B \widehat{\otimes} 1$ is mapped to itself identically, and $B = B \widehat{\otimes} g$ is mapped to $B_i g$ bijectively. Therefore ρ is an isomorphism. □

Let $K \leq_c G$, and let $M \in \mathbf{Mod}([\![RG]\!])$. Then M can be considered as an $[\![RK]\!]$-module. Sometimes it is advisable to emphasize, for clarity, that we are regarding M as an $[\![RK]\!]$-module and we write $\mathrm{res}_K^G(M)$, the *restriction of scalars* from G to K. With this notation we have,

Proposition 6.11.2 *Let G be a profinite group, H an open subgroup and K a closed subgroup of G. Assume that B is a profinite right $[\![RH]\!]$-module, where R is a commutative profinite ring. Then there exists an isomorphism of $[\![RK]\!]$-modules*

$$\mathrm{res}_K^G(\mathrm{Ind}_H^G(B)) \cong \bigoplus_{e\in E} \mathrm{Ind}_{K\cap e^{-1}He}^K \mathrm{res}_{K\cap e^{-1}He}^{e^{-1}He}(Be),$$

where E is a set of representatives of the set of double cosets $H\backslash G/K$.

Proof. Consider the decomposition (14) of $[\![RH]\!]$-modules. Since T is finite, the continuous action of K on T admits a continuous section. Denote by E the image of this section. Then E is a (finite) set of representatives of the space of double cosets $H\backslash G/K$, and K acts continuously on E. Therefore

$$\mathrm{Ind}_H^G(B) \cong \bigoplus_{e\in E}\Bigg(\bigoplus_{f\in e\cdot K} Bf\Bigg),$$

as $[\![RK]\!]$-modules. Since K acts on each orbit $e\cdot K$ continuously and transitively, and since the stabilizer of $f\in e\cdot K$ under the action of K is $K\cap e^{-1}He$, the result follows from Proposition 6.11.1. □

6.12 Notes, Comments and Further Reading

Most of the basic results on cohomology of profinite groups with discrete coefficient modules can be attributed to J. Tate. He has published almost nothing on this, but his work has been recorded in publications of Douady [1960], Lang [1966] and Serre [1995]. In our presentation we have built on the detailed exposition in Ribes [1970]. Brumer [1966] contains a good treatment of the Ext and Tor functors using pseudocompact modules over pseudocompact algebras; it also contains references to results about homology groups. The book of Serre [1995] contains in addition a treatment of nonabelian cohomology.

Lemma 6.7.9 was pointed out to us by Serre. Theorem 6.9.2 and its special case Theorem 6.9.3 are due to Schirokauer [1997] (in the context of profinite groups). The proof that we have presented here (Lemma 6.9.1 and Steps 2–4 of the proof that we give here of Theorem 6.9.3) is due to Serre. The original proof of Schirokauer is longer but very natural; he defines cohomology groups $H^n(G,A)$ of a profinite group G where the coefficient G-module A is allowed to be torsion profinite. He defines a transfer map $H^n(H,A)\longrightarrow H^n(G,A)$ for any closed subgroup H of G; using this, he obtains a decomposition as in Corollary 6.7.6, to reduce to the case when A is pro-p. Then he is able to use an argument similar to the one we use in Step 1 of the proof presented here. Theorem 6.9.2 is a generalization of a result of Gaschütz [1952] for finite groups.

The abstract version of Theorems 6.10.5 (and 6.10.9), which we call Shapiro's Lemma, is sometimes attributed also to B. Eckmann and to D.K. Faddeev. For a study of double coset formulas for profinite groups, see Symonds [2008].

Accounts of (co)homology of abstract groups can be found in Serre [1968], [1971], Lang [1966], Bieri [1976], Gruenberg [1970] and Brown [1982]. For homology in relation with p-adic analytic groups, see Symonds and Weigel [2000].

The following question is due to P.H. Kropholler.

Open Question 6.12.1 *Let G be a solvable pro-p group such that $H^n(G, \mathbf{Z}/p\mathbf{Z})$ is finite for every n. Is G polycyclic?*

7 Cohomological Dimension

7.1 Basic Properties of Dimension

Let G be a profinite group and let p be a prime number. Recall that if A is an abelian group, then A_p denotes its p-primary component, i.e., the subgroup consisting of those elements of A of order p^n, for some n. If $A = A_p$ we say that A is p-primary. The *cohomological p-dimension* $cd_p(G)$ of G is the smallest non-negative integer n such that $H^k(G, A)_p = 0$ for all $k > n$ and $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$, if such an n exists. Otherwise we say that $cd_p(G) = \infty$.

Similarly, the *strict cohomological p-dimension* $scd_p(G)$ of G is the smallest non-negative number n such that $H^k(G, A)_p = 0$ for all $k > n$ and $A \in \mathbf{DMod}(G)$.

Define

$$cd(G) = \sup_p cd_p(G),$$

and

$$scd(G) = \sup_p scd_p(G).$$

The next proposition is an obvious consequence of these definitions.

Proposition 7.1.1 *Let G be a profinite group and let n be a fixed natural number. The following statements are equivalent*

(a) $cd_p(G) \leq n$ (*respectively*, $scd_p(G) \leq n$);
(b) $H^k(G, A)_p = 0$ *for all* $k > n$ *and* $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$ (*respectively, for all* $k > n$ *and* $A \in \mathbf{Mod}(G)$).

Proposition 7.1.2 *Let G be a profinite group and let p be a prime. Then*

$$cd_p(G) \leq scd_p(G) \leq cd_p(G) + 1.$$

Proof. The first inequality is clear. For the second we may suppose that $cd_p(G) < \infty$. Let $n = cd_p(G) + 1$. Assume $A \in \mathbf{Mod}(G)$ and let $p : A \longrightarrow A$ be multiplication by p. Denote the kernel of this map $A[p]$; in other words,

$$A[p] = \{a \in A \mid pa = 0\}.$$

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4_7,

Consider the short exact sequences

$$0 \longrightarrow A[p] \longrightarrow A \stackrel{p}{\longrightarrow} pA \longrightarrow 0,$$
$$0 \longrightarrow pA \longrightarrow A \longrightarrow A/pA \longrightarrow 0.$$

Then $A[p]$ and A/pA are in $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$, in fact they are annihilated by p. So, if $k \geq n$,

$$H^k(G, A[p]) = H^k(G, A/pA) = 0.$$

Therefore, from the long exact sequences corresponding to the short exact sequences above,

$$\cdots \longrightarrow H^k(G, A[p]) \longrightarrow H^k(G, A) \stackrel{\varphi}{\longrightarrow} H^k(G, pA) \longrightarrow \cdots$$
$$\cdots \longrightarrow H^{k-1}(G, A/pA) \longrightarrow H^k(G, pA) \stackrel{\psi}{\longrightarrow} H^k(G, A) \longrightarrow \cdots,$$

one obtains that the maps φ and ψ are injections if $k > n$. Hence their composition

$$\psi\varphi : H^k(G, A) \longrightarrow H^k(G, A)$$

is again an injection. On the other hand, it is clear that $\psi\varphi$ is multiplication by p. Thus

$$H^k(G, A)_p = 0, \quad \text{if } k > n.$$

Hence the second inequality follows. □

Example 7.1.3 Let $G = \widehat{\mathbf{Z}}$. As we shall see later (Theorem 7.7.4), for every p, we have $cd_p(G) = 1$. Consider $\mathbf{Q}$ as a G-module with trivial action. By Corollary 6.7.5, $H^n(G, \mathbf{Q}) = 0$ for $n \geq 1$. So, from the exact sequence

$$0 \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Q} \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0,$$

one obtains isomorphisms

$$H^{n+1}(G, \mathbf{Z}) \cong H^n(G, \mathbf{Q}/\mathbf{Z}) \quad (n \geq 1).$$

In particular $H^2(G, \mathbf{Z}) \cong H^1(G, \mathbf{Q}/\mathbf{Z}) = \mathrm{Hom}(\widehat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) = \mathbf{Q}/\mathbf{Z}$. Thus $scd_p(G) = 2$.

A G-module S is *simple* if it has precisely two submodules, the module itself and the zero submodule. Observe that a simple p-primary G-module S is annihilated by p, i.e., $pS = 0$. Our next proposition simplifies the problem of finding the cohomological p-dimension of a group.

Proposition 7.1.4 *Let G be a profinite group and let n be a fixed natural number. The following conditions are equivalent*:

(a) $cd_p(G) \leq n$;
(b) $H^k(G, A) = 0$ *for all $k > n$ and all p-primary $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$*;

(c) $H^{n+1}(G, A) = 0$ *for all simple* p*-primary* G*-modules* $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$;
(d) $\mathrm{Ext}^{n+1}_{[\![\mathbf{F}_pG]\!]}(\mathbf{F}_p, A) = 0$ *for all* $A \in \mathbf{DMod}([\![\mathbf{F}_pG]\!])$;
(e) *There exists a projective resolution*

$$0 \to P_n \to P_{n-1} \to \cdots \to P_0 \to \mathbf{F}_p \to 0$$

of $\mathbf{F}_p$ *in* $\mathbf{PMod}([\![\mathbf{F}_pG]\!])$ *of length* n;
(f) *If*

$$0 \to L_n \to L_{n-1} \to \cdots \to L_0 \to \mathbf{F}_p \to 0$$

is an exact sequence in $\mathbf{PMod}([\![\mathbf{F}_pG]\!])$ *and* L_i *is projective for* $0 \le i \le n-1$, *then* L_n *is projective.*

Proof. The implications (a) $\Rightarrow$ (b) $\Rightarrow$ (c) are clear.

(c) $\Rightarrow$ (d): By Remark 6.2.5,

$$H^{n+1}(G, A) = \mathrm{Ext}^{n+1}_{[\![\widehat{\mathbf{Z}}G]\!]}(\widehat{\mathbf{Z}}, A) \cong \mathrm{Ext}^{n+1}_{[\![\mathbf{F}_pG]\!]}(\mathbf{F}_p, A),$$

for all $[\![\mathbf{F}_pG]\!]$-modules A, i.e., for all $[\![\widehat{\mathbf{Z}}G]\!]$-modules which are annihilated by p. By Lemma 5.1.1(a) and Corollary 6.1.8(a), to prove that $\mathrm{Ext}^{n+1}_{[\![\mathbf{F}_pG]\!]}(\mathbf{F}_p, A) = 0$, we may assume that A is a finite $[\![\mathbf{F}_pG]\!]$-module. For such a finite module $A \neq 0$, consider a series

$$0 = A_0 < A_1 < \cdots < A_t = A$$

where A_i is a submodule of A and the quotient A_{i+1}/A_i is a simple module ($i = 0, \dots, t-1$). We say that t is the *length* of A. If $t = 1$, the result holds by part (c). Let A be a finite $[\![\mathbf{F}_pG]\!]$-module of length $t > 1$ and assume that the result holds for $[\![\mathbf{F}_pG]\!]$-modules of length at most $t-1$. Consider the short exact sequence

$$0 \longrightarrow A_{t-1} \longrightarrow A \longrightarrow A/A_{t-1} \longrightarrow 0.$$

From the long exact sequence associated with the cohomological functor $\{\mathrm{Ext}^r_{[\![\mathbf{F}_pG]\!]}(\mathbf{F}_p, -)\}_{r\in\mathbf{N}}$ and the above short exact sequence (see Proposition 6.1.7(a)) we deduce that $\mathrm{Ext}^{n+1}_{[\![\mathbf{F}_pG]\!]}(\mathbf{F}_p, A) = 0$, as needed.

(d) $\Leftrightarrow$ (e) $\Leftrightarrow$ (f): Put $R = [\![\mathbf{F}_pG]\!]$. The equivalence of these three statements is well-known and, in fact, it is valid for any ring. The implications (f) $\Rightarrow$ (e) $\Rightarrow$ (d) are obvious. Here we prove that (d) $\Rightarrow$ (f). Consider the exact sequence in part (f), and define short exact sequences

$$0 \to K_{i+1} \to L_i \to K_i \to 0,$$

where $K_{i+1} = \mathrm{Ker}(L_i \to L_{i-1}) = \mathrm{Im}(L_{i+1} \to L_i)$. Remark that $L_n = K_n$. Correspondingly, there are long exact sequences,

$$\mathrm{Ext}^k_R(L_i, A) \to \mathrm{Ext}^k_R(K_{i+1}, A) \xrightarrow{\delta_i^k} \mathrm{Ext}^{k+1}_R(K_i, A) \to \mathrm{Ext}^{k+1}_R(L_i, A) \to \cdots,$$

where δ_i^k is the connecting homomorphism. Note that $\mathrm{Ext}_R^k(L_i, A) = 0$ whenever L_i is projective and $k \geq 1$. Hence δ_i^k is an isomorphism for $0 \leq i \leq n-1$ and $k \geq 1$. Thus the composite map

$$\delta = \delta_0^n \cdots \delta_{n-1}^1 : \mathrm{Ext}_R^1(L_n, A) = \mathrm{Ext}_R^1(K_n, A) \cong \mathrm{Ext}_R^{n+1}(\mathbf{F}_p, A)$$

is an isomorphism.

It follows from (d) and the hypotheses of (f), that $\mathrm{Ext}_R^1(L_n, A) = 0$, for all A. One deduces that $\mathrm{Ext}_R^0(L_n, -) = \mathrm{Hom}_R(L_n, -)$ is an exact functor. Therefore, L_n is projective (see Section 5.4); thus (f) holds.

(d) $\Rightarrow$ (c): This is clear since every simple p-primary G-module is annihilated by p, and so it is in $\mathbf{DMod}([\![\mathbf{F}_p G]\!])$.

(b) $\Rightarrow$ (a): Let $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$. Then $A = \bigoplus_p A_p$ is a decomposition of discrete $[\![\widehat{\mathbf{Z}}G]\!]$-modules. So (see Corollary 6.5.6),

$$H^k(G, A) = \bigoplus_p H^k(G, A_p).$$

Hence

$$H^k(G, A)_p \cong H^k(G, A_p).$$

Thus if $k > n$, we have $H^k(G, A)_p = 0$, and hence $cd_p(G) \leq n$.

(c) $\Rightarrow$ (b): Assume first that A is a finite p-primary $[\![\widehat{\mathbf{Z}}G]\!]$-module. We shall show, by induction on the order of A, that $H^{n+1}(G, A) = 0$. If $A = 0$, this is obviously true. If $A \neq 0$, assume true for those modules of order less than $|A|$. Let A' be a simple G-module contained in A. Consider the exact sequence

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A/A' \longrightarrow 0,$$

and its corresponding long exact sequence

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

Since $H^{n+1}(G, A') = H^{n+1}(G, A/A') = 0$, one has $H^{n+1}(G, A) = 0$.

Now we prove that $H^{n+1}(G, A) = 0$ for all p-primary $A \in \mathbf{DMod}(G)$. By Lemma 5.1.1

$$A \cong \varinjlim A_i,$$

where A_i runs through all the finite submodules of A. So (see Corollary 6.5.6),

$$H^{n+1}(G, A) \cong \varinjlim H^{n+1}(G, A_i) = 0. \tag{1}$$

It remains to prove that $H^k(G, A) = 0$ for all $k > n$ and all p-primary $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$. Let $k \geq n$. Consider the exact sequence

$$0 \longrightarrow A \stackrel{\iota}{\longrightarrow} \mathrm{Coind}_1^G(A) \longrightarrow A' \longrightarrow 0$$

of G-modules, where $\iota(a)(x) = xa$ ($a \in A$, $x \in G$) and $A' = \mathrm{Coind}_1^G(A)/\iota(A)$. From the corresponding long exact sequence

$$\cdots \to H^k(G, A') \xrightarrow{\delta} H^{k+1}(G, A) \to H^{k+1}(G, \mathrm{Coind}_1^G(A)) \to \cdots$$

and the fact that $H^t(G, \mathrm{Coind}_1^G(A)) = 0$ if $t \geq 1$ (see Corollary 6.10.6), we obtain

$$H^k(G, A') \cong H^{k+1}(G, A)$$

for $k \geq 1$. By an induction argument on k, we deduce from (1) that $H^k(G, A) = 0$ for $k > n$. □

For pro-p groups, the simple p-primary modules are particularly convenient and easy to describe. In fact there is only one such a module, as shown in the following

Lemma 7.1.5 *If G is a pro-p group, every discrete simple p-primary G-module A is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ (where the abelian group $\mathbf{Z}/p\mathbf{Z}$ is considered as a G-module on which G operates trivially).*

Proof. Since A is simple and p-primary, it follows from Lemma 5.1.1 that A is finite of order a power of p. Furthermore $pA = 0$, since pA is a G-submodule of A. Put $U = \bigcap_{a \in A} U_a$, where U_a is the stabilizer of a. Since each U_a is open (see Lemma 5.3.1), so is U. Let $V = \bigcap_{t \in G/U} t^{-1}Ut$ be the core of U in G. Then V is a normal open subgroup of G, and V acts trivially on A. So the finite p-group G/V acts naturally on A, and A is a simple G/V-module. Thus we may assume that G is finite.

Claim that G acts trivially on A. Suppose not; then $A^G = 0$, because A is simple. Write A as the disjoint union of its orbits under the action of G. Then the cardinality of each of these orbits is divisible by p, except for the orbit of 0 which has cardinality 1. It follows that $|A| \equiv 1$ modulo p, contradicting the fact that $|A|$ is a power of p. This proves the claim. Finally, since $\mathbf{Z}/p\mathbf{Z}$ is the only simple abelian group of exponent p, we have $A \cong \mathbf{Z}/p\mathbf{Z}$. □

Combining this lemma with Proposition 7.1.4, we obtain the following useful characterization of cohomological dimension for pro-p groups.

Corollary 7.1.6 *Let G be a pro-p group and let n be a fixed natural number. Then $cd(G) \leq n$ if and only if $H^{n+1}(G, \mathbf{Z}/p\mathbf{Z}) = 0$.*

Corollary 7.1.7 *If G is a pro-p group and $cd(G) = n$, then $H^n(G, A) \neq 0$ for every finite p-primary discrete G-module $A \neq 0$.*

Proof. Let A be a finite p-primary discrete G-module. By Lemma 7.1.5, there exists some G-submodule K of A such that $A/K \cong \mathbf{Z}/p\mathbf{Z}$. Construct an exact sequence of G-modules of the form

$$0 \longrightarrow K \longrightarrow A \xrightarrow{f} \mathbf{Z}/p\mathbf{Z} \longrightarrow 0.$$

The corresponding long exact sequence in cohomology

$$\cdots \longrightarrow H^n(G,A) \xrightarrow{\bar{f}} H^n(G,\mathbf{Z}/p\mathbf{Z}) \longrightarrow H^{n+1}(G,K) = 0$$

shows that $\bar{f}$ is onto. So, since $H^n(G,\mathbf{Z}/p\mathbf{Z}) \neq 0$, we have $H^n(G,A) \neq 0$. □

7.2 The Lyndon-Hochschild-Serre Spectral Sequence

Throughout this section G is a profinite group and K a closed normal subgroup of G. Our aim is to obtain a spectral sequence that relates the (co)homology groups of G, K and G/K. We consider cohomology groups first, and we shall work with coefficient modules for the cohomology of G which are discrete G-modules, not necessarily torsion. The corresponding results for homology will be obtained by restricting ourselves to torsion modules and dualizing.

Let $A \in \mathbf{DMod}(G)$. Define $C_K^n(G,A)$ to be the discrete abelian group consisting of all continuous maps $f : G^{n+1} \longrightarrow A$ such that

$$f(kx_0,\ldots,kx_n) = kf(x_0,\ldots,x_n) \quad (k \in K, x_0,\ldots,x_n \in G).$$

Define

$$\partial = \partial^{n+1} : C_K^n(G,A) \longrightarrow C_K^{n+1}(G,A)$$

by

$$(\partial^{n+1}f)(x_0,\ldots,x_{n+1}) = \sum_{i=0}^{n+1}(-1)^i f(x_0,\ldots,\hat{x}_i,\ldots,x_{x+1})$$

(the symbol $\hat{x}_i$ indicates, as usual, that x_i is to be omitted). Then $\partial^{n+1}\partial^n = 0$ $(n \geq 1)$, so that

$$(\mathbf{C}_K(G,A),\partial) : \cdots \to C_K^n(G,A) \xrightarrow{\partial} C_K^{n+1}(G,A) \to \cdots$$

is a complex.

Lemma 7.2.1 *$H^n(K,A) \cong H^n(\mathbf{C}_K(G,A),\partial)$.*

Proof. Remark that this is clear if we assume that A is torsion, for then it follows from the fact that the G-resolution (1) in Section 6.2 is a free K-resolution as well. Here we give a computational proof valid for any G-module. Taking into account Definition 6.4.1 and Shapiro's lemma (see Theorem 6.10.5), it suffices to show that the complexes $\mathbf{C}(G,\mathrm{Coind}_K^G(A))$ and $\mathbf{C}_K(G,A)$ are isomorphic. In order to prove this, define homomorphisms

$$C_K^n(G,A) \xrightarrow{\Phi^n} C^n(G,\mathrm{Coind}_K^G(A)) \quad \text{and} \quad C^n(G,\mathrm{Coind}_K^G(A)) \xrightarrow{\Psi^n} C_K^n(G,A)$$

by

$$(\Phi^n f)(x_0,\ldots,x_n)(x) = f(xx_0,\ldots,xx_n);$$

and

$$(\Psi^n g)(x_0,\ldots,x_n) = g(x_0,\ldots,x_n)(1),$$

($f \in C_K^n(G,A); g \in C^n(G, \mathrm{Coind}_K^G(A)); x, x_i \in G$). Then it is easily verified that $\{\Phi^n\}_{n\in\mathbf{N}}$ and $\{\Psi^n\}_{n\in\mathbf{N}}$ are morphisms of complexes (i.e., they commute with the maps ∂), and they are inverse to each other. □

We consider each $C_K^n(G,A)$ as a G/K-module by means of the following action. Let

$$x \in G \quad \text{and} \quad f \in C_K^n(G,A);$$

put $\bar{x} = xK$; then $\bar{x}f : G^{n+1} \longrightarrow A$ is defined by

$$(\bar{x}f)(x_0,\ldots,x_n) = xf(x^{-1}x_0,\ldots,x^{-1}x_n).$$

Note that this is well-defined. From the continuity of f one deduces that $\bar{x}f$ is also continuous. Using the normality of K in G, we have

$$\begin{aligned}(\bar{x}f)(kx_0,\ldots,kx_n) &= xf(x^{-1}kx_0,\ldots,x^{-1}kx_n)\\ &= xf(x^{-1}kxx^{-1}x_0,\ldots,x^{-1}kxx^{-1}x_n)\\ &= k(\bar{x}f)(x_0,\ldots,x_n).\end{aligned}$$

Hence $\bar{x}f \in C_K^n(G,A)$. Moreover the action of G/K on $C_K^n(G,A)$ is continuous, therefore $C_K^n(G,A) \in \mathbf{DMod}(G/K)$. Since

$$\partial^{n+1}(\bar{x}f) = \bar{x}(\partial^{n+1}f)$$

($n \in \mathbf{N}, x \in G, f \in C_K^n(G,A)$), the groups $H^n(K,A)$ are also G/K-modules.

Remark 7.2.2 It is sometimes more convenient to describe the action of G/K on $H^n(K,A)$ in terms of nonhomogeneous cochains. We claim that the action defined above is precisely the following: let $f \in C^n(K,A)$ be a cochain representing an element of $H^n(K,A)$, and assume that $x \in G$ and $k_1,\ldots,k_n \in K$. Then

$$(\bar{x}f)(k_1,\ldots,k_n) = xf(x^{-1}k_1x,\ldots,x^{-1}k_nx).$$

To verify this, note that multiplication by $\bar{x}$ determines automorphisms of the cohomological functors (on the variable $A \in \mathbf{DMod}(G)$)

$$H^\bullet(\mathbf{C}_K(G,A)) \quad \text{and} \quad H^\bullet(K,A).$$

Hence, it suffices to see that the two actions that we have defined coincide on dimension zero (after we identify $H^0(\mathbf{C}_K(G,A))$ with $H^0(K,A)$ via the isomorphism given in Lemma 7.2.1). An element of $H^0(K,A)$ can be represented by a constant function $f : K \longrightarrow A$ given by $f(k) = a$, for all $k \in K$, where a is an element of A^K. The corresponding element of $H^0(\mathbf{C}_K(G,A))$

can be represented by the constant function $\bar{f} : G \longrightarrow A$ given by $\bar{f}(y) = a$, for all $y \in G$. Now, according to our definitions,

$$(\bar{x}\bar{f})(y) = x\bar{f}(x^{-1}y) = xa,$$

and

$$(\bar{x})f(k) = xf(x^{-1}kx) = xa.$$

Finally, the elements of $H^0(\mathbf{C}_K(G, A)$ and $H^0(K, A)$ represented by the constant functions with value xa, correspond to each other under the isomorphism given in Lemma 7.2.1. Thus the assertion is proved.

Next we shall construct a double complex using the complexes $\mathbf{C}_K(G, -)$ and $\mathbf{C}(G/K, -)$; then, following standard techniques (see Appendix A, Section A.4) we build a spectral sequence relating the cohomology of the groups G, K and G/K. Define a double complex $\mathbf{L} = (L^{r,s}, \partial', \partial'')$ by

$$L^{r,s} = C^r(G/K, C_K^s(G, A))$$

where

$$\partial' : C^r(G/K, C_K^s(G, A)) \longrightarrow C^{r+1}(G/K, C_K^s(G, A))$$

is induced by

$$\partial^{r+1} : C^r(G/K, -) \longrightarrow C^{r+1}(G/K, -)$$

and

$$\partial'' : C^r(G/K, C_K^s, (G, A)) \longrightarrow C^r(G/K, C_K^{s+1}(G, A))$$

is induced by

$$(-1)^r \partial^{s+1} : C_K^s(G, -) \to C_K^{s+1}(G, -).$$

Clearly $\partial'\partial' = 0$, $\partial''\partial'' = 0$ and $\partial'\partial' + \partial''\partial'' = 0$.

Lemma 7.2.3 *$H^s(G/K, C_K^r(G, A)) = 0$, if $s > 0$.*

Proof. Consider $f \in C_K^s(G/K, C^r(G, A))$ with $\partial^{s+1}(f) = 0$. Define

$$g \in C^{s-1}(G/K, C_K^r(G, A))$$

by

$$g(\bar{x}_0, \ldots, \bar{x}_{s-1})(y_0, \ldots, y_r) = f(\bar{x}_0, \ldots, \bar{x}_{s-1}, \bar{y}_0)(y_0, \ldots, y_r) \quad (x_i, y_j \in G).$$

Then one readily checks that $\partial^s((-1)^s g) = f$. □

In the following theorem a very useful spectral sequence is constructed. It is the counterpart of the Lyndon-Hochschild-Serre spectral sequence for abstract groups.

Theorem 7.2.4 *Let K be a normal closed subgroup of a profinite group G, and let $A \in \mathbf{DMod}(G)$. Then there exists a spectral sequence $\mathbf{E} = (E_t^{r,s})$ such that*

$$E_2^{r,s} \cong H^r(G/K, H^s(K, A))$$

and

$$E_2^{r,s} \Rightarrow H^n(G, A).$$

Proof. We shall show that $\mathbf{E}$ is the first spectral sequence of the double complex

$$L^{r,s} = (C^r(G/K, C_K^s(G, A)), \partial', \partial'').$$

We shall make use of the second spectral sequence of this double complex to show that $\mathbf{E}$ converges to $H^n(G, A)$.

By the results in Section A.4, we have

$$'E_1^{r,s} \cong H^s(L^{r,\bullet}) = H^s(C^r(G/K, C_K^\bullet(G, A)), \partial'').$$

Since $C^r(G/K, -)$ is an exact functor (see Lemma 6.5.4), we obtain

$$'E_1^{r,s} \cong C^r(G/K, H^s(K, A)).$$

From this we get

$$'E_2^{r,s} \cong H^r(G/K, H^s(K, A)).$$

This spectral sequence converges to $H^n(\mathrm{Tot}(\mathbf{L}))$ (see Theorem A.4.1). To compute $H^n(\mathrm{Tot}(\mathbf{L}))$, we consider the second spectral sequence of the double complex $\mathbf{L}$. We have

$$''E_1^{r,s} \cong H^s(L^{\bullet,r}) = H^s(G/K, C_K^r(G, A)).$$

By Lemma 7.2.3, $''E_1^{r,s} = 0$, for $s > 0$. Hence the second spectral sequence of $\mathbf{L}$ collapses, i.e., $''E_t^{r,s} = 0$, for $s > 0$ and $1 \le t \le \infty$. Since

$$''F^r H^n(\mathrm{Tot}(\mathbf{L}))/''F^{r+1} H^n(\mathrm{Tot}(\mathbf{L})) = ''E_\infty^{r,s} = 0$$

if $r + s = n$, $s > 0$, we have

$$''E_\infty^{n,0} \cong ''F^n H^n(\mathrm{Tot}(\mathbf{L})) \cong ''F^{n-1} H^n(\mathrm{Tot}(\mathbf{L})) \cong \cdots \cong H^n(\mathrm{Tot}(\mathbf{L})).$$

On the other hand $''E_2^{n,0} \cong ''E_\infty^{n,0}$. Thus

$$\begin{aligned} H^n(\mathrm{Tot}(\mathbf{L})) &\cong ''E_2^{n,0} \cong H^n(H^0(L^{\bullet,i}), \partial'') \cong H^n(H^0(G/K, C_K^\bullet(G, A)), \partial'') \\ &\cong H^n(C_K^\bullet(G, A)^{G/K}, \partial) \cong H^n(C^\bullet(G, A), \partial) \cong H^n(G, A). \end{aligned}$$ □

Corollary 7.2.5 *Let G be a profinite group, K a closed normal subgroup of G and $A \in \mathbf{DMod}(G)$.*

(a) *Assume* $H^s(K,A)=0$ *for* $0<s<n$. *Then we obtain a five term exact sequence*

$$0\to H^n(G/K,A^K)\xrightarrow{\text{Inf}} H^n(G,A)\xrightarrow{\text{Res}} H^n(K,A)^{G/K} \xrightarrow{\text{tr}} H^{n+1}(G/K,A^K)\xrightarrow{\text{Inf}} H^{n+1}(G,A).$$

(b) *In particular, there exists always a five term exact sequence*

$$0\longrightarrow H^1(G/K,A^K)\xrightarrow{\text{Inf}} H^1(G,A) \xrightarrow{\text{Res}} H^1(K,A)^{G/K}\xrightarrow{\text{tr}} H^2(G/K,A^K)\xrightarrow{\text{Inf}} H^2(G,A).$$

Proof. This follows from Theorem A.2.6 applied to the Lyndon-Hochschild-Serre spectral sequence. □

Dualizing part (b) of the above corollary, one obtains,

Corollary 7.2.6 *Let* G *be a profinite group,* K *a closed normal subgroup of* G *and* $B\in \mathbf{PMod}([\![\widehat{\mathbf{Z}}G]\!])$. *Then, there exists a five term exact sequence of homology groups*

$$H_2(G,B)\longrightarrow H_2(G/K,B_K)\longrightarrow H_1(K,B)_{G/K} \longrightarrow H_1(G,B)\longrightarrow H_1(G/K,B_K)\longrightarrow 0.$$

As an application of the five term exact sequence in the above corollaries we obtain the following criterion.

Proposition 7.2.7 *Let*

$$1\longrightarrow K\longrightarrow G\xrightarrow{\varphi} H\longrightarrow 1$$

be an exact sequence of prosolvable groups. Assume that for each simple discrete $[\![\widehat{\mathbf{Z}}H]\!]$*-module* A *one has*

(1)

$$\text{Inf}: H^1(H,A)\longrightarrow H^1(G,A)$$

is an epimorphism, and

(2)

$$\text{Inf}: H^2(H,A)\longrightarrow H^2(G,A)$$

is a monomorphism.

Then φ *is an isomorphism.*

Proof. The action of G on A is defined via φ, by $xa = \varphi(x)a$ $(x \in G, a \in A)$. Hence K act trivially on A, so that the maps in the statement are indeed inflation maps. Consider the five term exact sequence of Corollary 7.2.5,

$$0 \longrightarrow H^1(H,A) \longrightarrow H^1(G,A) \longrightarrow H^1(K,A)^H \longrightarrow H^2(H,A) \longrightarrow H^2(G,A).$$

By our assumptions, $H^1(K,A)^H = 0$. We have to prove that $K = 1$. Suppose that $K \neq 1$. Then there exists $U \triangleleft_o G$ such that $K \cap U \neq K$. Since $K/K\cap U$ is a finite nontrivial solvable group, there exists $W \triangleleft_o K$ such that $W \geq K \cap U$ and K/W is a finite nontrivial abelian group. Let W_G be the core of W in G. Then K/W_G is a finite nontrivial abelian group and $W_G \triangleleft_o G$. Therefore, there exists some closed subgroup V of G which is maximal with respect to the following properties

$$V \triangleleft_o K \quad \text{and} \quad K/V \quad \text{is nontrivial abelian.}$$

Let G act on K/V on the left by 'conjugation':

$$x \cdot (kV) = xkx^{-1}V \quad (x \in G, k \in K).$$

Note that K/V is a finite simple discrete G-module, and that the induced action of K on K/V is trivial. Hence K/V becomes an H-module in a natural way. Clearly K/V is simple as an H-module. Therefore,

$$H^1(K, K/V)^H = 0.$$

Since K/V is a trivial K-module, we have

$$H^1(K, K/V) = \mathrm{Hom}(K, K/V).$$

Let $f : K \longrightarrow K/V$ be the canonical epimorphism $k \mapsto kV$. We claim that $f \in H^1(K, K/V)^H$. Indeed (see Remark 7.2.2), if $x \in G$ and $k \in K$, one has

$$(\bar{x}f)(k) = x \cdot f(x^{-1}kx) = x \cdot (x^{-1}kxV) = xx^{-1}kxx^{-1}V = kV = f(k),$$

so that $\bar{x}f = f$. Thus $f = 0$, i.e., $K = V$, a contradiction. This proves the claim and the proposition. □

7.3 Cohomological Dimension of Subgroups

This section contains results relating the p-cohomological dimension of a profinite group and its closed subgroups.

Theorem 7.3.1 *Let G be a profinite group, H a closed subgroup of G and p a prime number. Then*

(a) $cd_p(H) \leq cd_p(G)$,

(b) $scd_p(H) \le scd_p(G)$.

Moreover, equality holds in either of the following cases

(1) $p \nmid [G : H]$,
(2) $cd_p(G) < \infty$ *and the exponent of* p *in the supernatural number* $[G : H]$ *is finite* (*this is the case, e.g., if* H *is open in* G).

Proof. We give proofs for the case of cohomological dimension; the case of strict cohomological dimension is analogous.

(a) Let $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}H]\!])$ and let $k > cd_p(G)$. Using Shapiro's lemma (see Theorem 6.10.5) we get

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

as desired.

(1) Let $n \ge 1$ be such that there exists $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$ with $H^n(G, A)_p \ne 0$. By Corollary 6.7.7,

$$\mathrm{Res} : H^k(G, A)_p \longrightarrow H^k(H, A)_p$$

is an injection if $k \ge 1$, since $p \nmid [G : H]$. Therefore

$$H^n(H, A)_p \ne 0.$$

Hence $cd_p(H) \ge cd_p(G)$. By part (a) we obtain equality.

(2) First we consider the case that H is open. Let $cd_p(G) = n$ be finite. Then there exists $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$ with $H^n(G, A)_p \ne 0$. Choose a right transversal $\{t_i\}_{i \in I}$ of H in G containing 1. Define homomorphisms

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

and

$$A \xrightarrow{\iota} \mathrm{Coind}_H^G(A)$$

by

$$\pi(f) = \sum_{i \in I} t_i^{-1} f(t_i) \quad f \in \mathrm{Coind}_H^G(A)$$

and, for $a \in A$, $x \in G$,

$$(\iota(a))(x) = \begin{cases} xa & \text{if } x \in H \\ 0 & \text{if } x \in G - H. \end{cases}$$

Then $\pi\iota = \mathrm{id}_A$. So π is surjective. One verifies easily that π is a G-homomorphism. Let $A' = \mathrm{Ker}(\pi)$. Consider the exact sequence

$$0 \longrightarrow A' \longrightarrow \mathrm{Coind}_H^G(A) \xrightarrow{\pi} A \longrightarrow 0.$$

From the corresponding long exact sequence in cohomology we obtain that

$$H^n(G, \mathrm{Coind}_H^G(A))_p \xrightarrow{\bar{\pi}} H^n(G, A)_p \xrightarrow{\delta} H^{n+1}(G, A')_p$$

is exact. Since $H^{n+1}(G, A')_p = 0$, $\bar{\pi}$ is surjective. Hence, since $H^n(G, A)_p \neq 0$,

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

Therefore, by Shapiro's lemma (see Theorem 6.10.5),

$$H^n(H, A) \neq 0.$$

Thus $cd_p(H) \geq n$. Equality follows then from part (a). This proves the statement when H is open.

Assume now that p has finite exponent, say t, in $[G : H]$. Choose p-Sylow subgroups G_p of G and H_p of H such that $H_p \leq G_p$. Let U be an open normal subgroup of G. Then $[G_pU/U : H_pU/U] \leq p^t$. Hence $[G_p : H_p] = p^t$, finite. By the above case, $cd_p(G_p) = cd_p(H_p)$. On the other hand, by part (1), $cd_p(H_p) = cd_p(H)$ and $cd_p(G_p) = cd_p(G)$. Thus $cd_p(H) = cd_p(G)$. □

Remark 7.3.2 The condition $cd_p(G) < \infty$ in part (2) above is necessary. For example, if G is a finite p-group, then it is well-known that $cd_p(G) = \infty$ (cf. Cartan and Eilenberg [1956], page 255), while $cd_p(1) = 0$.

For an example involving infinite groups, let

$$G = G_{\mathbf{Q}} \quad \text{and} \quad H = G_{\mathbf{Q}(i)}$$

be the absolute Galois groups of the fields $\mathbf{Q}$ and $\mathbf{Q}(i)$, respectively. Then (cf. Ribes [1970], Theorem V.8.8)

$$cd_2(G) = \infty \quad \text{and} \quad cd_2(H) = 2.$$

Corollary 7.3.3 *Let G_p be a p-Sylow group of a profinite group G. Then*

(a) $cd_p(G) = cd_p(G_p) = cd(G_p)$,
(b) $scd_p(G) = scd_p(G_p) = scd(G_p)$,
(c) $cd_p(G) = 0$ *if and only if* $p \nmid \#G$.

Proof. Parts (a) and (b) follow immediately from Theorem 7.3.1. To demonstrate part (c), we may assume that G is a pro-p group. In this case, if $p \nmid \#G$ then $G = 1$, and so $cd_p(G) = 0$. Conversely, assume $cd_p(G) = 0$. Then $H^1(G, A) = 0$ for all $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$. In particular $H^1(G, \mathbf{Z}/p\mathbf{Z}) = 0$, where $\mathbf{Z}/p\mathbf{Z}$ is considered as a trivial G-module. However,

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

the group of continuous homomorphisms. This clearly implies that $G = 1$, since every nontrivial pro-p group has an open normal subgroup of index p. □

Corollary 7.3.4 *If $cd_p(G) \neq 0, \infty$, then p^∞ divides $\#G$.*

Proof. By Corollary 7.3.3, we may assume that G is a pro-p group and $G \neq 1$. Observe that G is infinite, for otherwise $cd_p(G) = \infty$ (cf. Cartan and Eilenberg [1956], page 255). Thus $p^\infty \mid \#G$. □

Next we supplement Theorem 7.3.1 with a powerful result due to Serre that establishes the equality of the p-cohomological dimensions of a group and an open subgroup when the group has no p-torsion. We deduce this result from a theorem of Scheiderer which we only state here. We need first some notation.

Let G be a profinite group and express it as an inverse limit

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

where $\mathcal{U}$ is the set of all open normal subgroups of G. Denote by $\mathcal{S}$ (respectively, $\mathcal{S}_U$) the set of all closed subgroups of G (respectively, of $G_U = G/U$). Clearly

$$\mathcal{S} = \varprojlim_{U \in \mathcal{U}} \mathcal{S}_U.$$

Hence $\mathcal{S}$ can be thought of as a profinite space.

Lemma 7.3.5 *Let G be a profinite group having an open normal torsion-free subgroup H. Then*

(a) *The space $\mathcal{F}$ of subgroups of G of finite order is closed in the space $\mathcal{S}$ of all closed subgroups of G; in particular, $\mathcal{F}$ is a profinite space;*
(b) *Let n be a natural number. Then the space $\mathcal{S}_n$ of subgroups of G of order n is closed in the space $\mathcal{S}$ of all closed subgroups of G and so it is profinite;*
(c) *The subset $T = tor(G) - \{1\}$ of nontrivial torsion elements of G is closed in G.*

Proof. (a) Let $R \in \mathcal{F}$. Since H is torsion-free, $H \cap R = 1$. Hence $|R|$ divides $[G : H]$. For each $U \triangleleft_o G$, let $\mathcal{F}_U$ denote the set of all subgroups of G/U whose order divides $[G : H]$. Then, using the notation introduced above,

$$\mathcal{F} = \varprojlim_{U \in \mathcal{U}} \mathcal{F}_U \leq \varprojlim_{U \in \mathcal{U}} \mathcal{S}_U = \mathcal{S}.$$

(b) Let $\mathcal{S}_H$ denote the set of all subgroups of G/H and let $\mathcal{S}_{nH}$ denote the set of all subgroups of order n in G/H. Let

$$\varphi : \mathcal{S} \longrightarrow \mathcal{S}_H$$

be the projection map. Since H is torsion-free, $\varphi^{-1}(\mathcal{S}_{nH})$ consists of all subgroups of G of order n together with possibly some infinite subgroups. Hence,

$$\mathcal{S}_n = \mathcal{F} \cap \varphi^{-1}(\mathcal{S}_{nH}).$$

Since both $\mathcal{F}$ and $\varphi^{-1}(\mathcal{S}_{nH})$ are closed in $\mathcal{S}$, the result follows.

(c) Set $n = [G : H]$. Then $y^n = 1$ for all $y \in T$ since H is torsion-free. Let $x \in \bar{T}$; hence $x^n = 1$. Therefore, either $x \in T$ or $x = 1$. So, $tor(G) = T \cup \{1\}$ is a closed set. On the other hand H is an open neighborhood of 1 and $H \cap T = \emptyset$. Thus, T is closed. □

Let G be a profinite group and let p be a prime number. Consider the set $\mathcal{S}_p$ of all subgroups of G of order p; then, by the preceding lemma, $\mathcal{S}_p$ has in a natural way the structure of a profinite space. Observe that $\mathcal{S}_p$ is a right G-space by means of the natural action

$$\mathcal{S}_p \times G \longrightarrow \mathcal{S}_p$$

given by conjugation: $(S, g) \mapsto g^{-1}Sg$ $(S \in \mathcal{S}_p)$.

We can state now the following result (Scheiderer [1994]).

Theorem 7.3.6 *Let G be a profinite group which does not contain any subgroup isomorphic to $C_p \times C_p$, where p is a fixed prime number. Assume that H is an open subgroup of G of finite cohomological p-dimension d.*

(a) *Let A be a discrete p-primary left G-module. Then the natural homomorphism*

$$\varphi : A \longrightarrow \mathrm{C}(\mathcal{S}_p, A) = \mathrm{Hom}([\![\widehat{\mathbf{Z}}\mathcal{S}_p]\!], A)$$

that sends $a \in A$ to the constant map $\mathcal{S}_p \to A$ with value a, induces isomorphisms

$$\varphi^n : H^n(G, A) \longrightarrow H^n(G, \mathrm{C}(\mathcal{S}_p, A))$$

for every $n > d$.

Dually,

(b) *If B is a profinite p-primary right G-module, the natural homomorphism*

$$B\widehat{\otimes}[\![\widehat{\mathbf{Z}}\mathcal{S}_p]\!] \longrightarrow B$$

defined by $b\widehat{\otimes}\bar{t} \mapsto b\epsilon(\bar{t})$ $(b \in B,\ \bar{t} \in [\![\widehat{\mathbf{Z}}\mathcal{S}_p]\!])$, where $\epsilon : [\![\widehat{\mathbf{Z}}\mathcal{S}_p]\!] \longrightarrow \widehat{\mathbf{Z}}$ is the augmentation map, induces isomorphisms

$$H_n(G, B\widehat{\otimes}[\![\widehat{\mathbf{Z}}\mathcal{S}_p]\!]) \longrightarrow H_n(G, B)$$

for each $n > d$.

We now prove a result, due to Serre [1965], as a consequence of this theorem. Historically Serre's result precedes the above theorem by 30 years.

Theorem 7.3.7

(a) *Let G be a profinite group with no subgroups of order p, and let H be an open subgroup of G. Then*

$$cd_p(G) = cd_p(H).$$

(b) *Let G be a torsion-free pro-p group. If G is virtually a free pro-p group* (*i.e.*, *G contains an open subgroup which is a free pro-p group*), *then it is free pro-p.*

Proof. Part (b) is a consequence of part (a) and Theorem 7.7.4. To show part (a) notice first that if $cd_p(H) = \infty$, the result follows since $cd_p(H) \leq cd_p(G)$ (see Theorem 7.3.1). Assume then that $cd_p(H) = d$ is finite. Observe that in this case $\mathcal{S}_p = \emptyset$, and so $[\![\widehat{\mathbf{Z}}\mathcal{S}_p]\!] = 0$. It follows from Theorem 7.3.6 that

$$H^n(G, \mathbf{Z}/p\mathbf{Z}) = H^n(G, \mathrm{Hom}([\![\widehat{\mathbf{Z}}\mathcal{S}_p]\!], \mathbf{Z}/p\mathbf{Z})) = 0$$

if $n > d$. Therefore $cd_p(G) = d$. □

7.4 Cohomological Dimension of Normal Subgroups and Quotients

Here we study the relationship between the cohomology of a group and that of a normal subgroup and the corresponding quotient. The main tool again is the Lyndon-Hochschild-Serre spectral sequence.

Lemma 7.4.1 *Let G be a profinite group and K a closed normal subgroup of G. Assume $cd_p(G/K) = m$ and $cd_p(K) = n$ are finite. Then, for every prime p and each discrete G-module A,*

$$H^{n+m}(G, A)_p \cong H^m(G/K, H^n(K, A))_p.$$

Proof. Consider the Lyndon-Hochschild-Serre spectral sequence (see Theorem 7.2.4)

$$E_2^{r,s} = H^r(G/K, H^s(K, A)) \quad \Rightarrow \quad H^n(G, A).$$

If $r > m$, then $(E_2^{r,s})_p = 0$; and if $r < m$ and $r + s = m + n$, then $s > n$, so again $(E_2^{r,s})_p = 0$. Hence $(E_\infty^{r,s})_p = 0$ if $r + s = m + n$, $r \neq m$. Thus the induced filtration of $H^{m+n}(G, A)_p$ is trivial and

$$H^{m+n}(G, A)_p \cong (E_\infty^{m,n})_p.$$

Finally, one easily sees that $(E_2^{m,n})_p \cong (E_\infty^{m,n})_p$. □

Proposition 7.4.2 *Let K be a normal closed subgroup of a profinite group G and let p be a prime. Then*

(a)

$$cd_p(G) \leq cd_p(K) + cd_p(G/K).$$

(b) *Assume that $cd_p(G/K)$ is finite. Then*

$$cd_p(G) = cd_p(K) + cd_p(G/K)$$

in either of the following cases

(i) K *is a pro-p group with* $cd(K) = n$ *and* $H^n(K, \mathbf{Z}/p\mathbf{Z})$ *is finite*;
(ii) K *is in the center of* G.

Proof. (a) Consider the Lyndon-Hochschild-Serre spectral sequence

$$E_2^{r,s} = H^r(G/K, H^s(K, A)) \quad \Rightarrow \quad H^n(G, A).$$

Let $m > cd_p(K) + cd_p(G/K)$. We shall show that $H^m(G, A)_p = 0$ if $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$. Choose $r, s \geq 0$ such that $r + s = m$. Then either $s > cd_p(K)$ or $r > cd_p(G/K)$. So

$$(E_2^{r,s})_p = 0, \quad \text{if } r + s = m.$$

Therefore

$$(E_\infty^{r,s})_p = 0, \quad r + s = m.$$

Thus

$$H^m(G, A)_p = 0.$$

(b) We may assume that $cd_p(G)$ is finite. Say $cd_p(G/K) = m$ and $cd_p(K) = n$. Let G_p be a p-Sylow subgroup of G. Then G_pK/K is a p-Sylow subgroup of G/K. Put $H = G_pK$. Then

$$cd_p(H/K) = cd_p(G/K) = m.$$

By part (a),

$$cd_p(H) \leq cd_p(G) \leq m + n.$$

So, it will suffice to prove that

$$cd_p(H) = m + n.$$

We may assume that G/K is a pro-p group.

Case (i): Suppose that K is a pro-p group with $cd(K) = n$ and $H^n(K, \mathbf{Z}/p\mathbf{Z})$ finite.

By Lemma 7.4.1 and Corollary 7.1.7,

$$H^{n+m}(G, \mathbf{Z}/p\mathbf{Z}) \cong H^m(G/K, H^n(K, \mathbf{Z}/p\mathbf{Z})) \neq 0$$

since $H^n(K, \mathbf{Z}/p\mathbf{Z})$ is p-primary and finite by hypothesis.

Case (ii): Suppose now that K is in the center of G.

By the description of the action given in Remark 7.2.2, one sees that the group G/K acts trivially on $H^n(K, \mathbf{Z}/p\mathbf{Z})$. Since K is abelian, it is the direct sum of its Sylow subgroups K_p (see Proposition 2.3.8). By Corollary 7.1.6, $H^n(K_p, \mathbf{Z}/p\mathbf{Z}) \neq 0$. Using cochains one easily sees that $H^n(K_p, \mathbf{Z}/p\mathbf{Z})$ is a direct summand of $H^n(K, \mathbf{Z}/p\mathbf{Z})$, and so $H^n(K, \mathbf{Z}/p\mathbf{Z}) \neq 0$. Therefore, as a G/K-module, $H^n(K, \mathbf{Z}/p\mathbf{Z})$ is isomorphic to a direct sum $\bigoplus_I (\mathbf{Z}/p\mathbf{Z})$ where $I \neq \emptyset$. Thus we have

$$H^{n+m}(G, \mathbf{Z}/p\mathbf{Z}) \cong \bigoplus_I H^m(G/K, \mathbf{Z}/p\mathbf{Z}) \neq 0.$$

□

Exercise 7.4.3

(a) Let $A = \mathbf{Z}_p \oplus \overset{m}{\cdots} \oplus \mathbf{Z}_p$ be a free abelian pro-p group of finite rank m. Then $cd_p(A) = m$.

(b) Let $\mathbf{Z}_p/p^m\mathbf{Z}_p$ act on $B = \mathbf{Z}_p \oplus \overset{p^m}{\cdots} \oplus \mathbf{Z}_p$ (the direct sum of p^m copies of $\mathbf{Z}_p$) by permuting the summands in a natural way and let $\mathbf{Z}_p$ act on B via the canonical epimorphism

$$\mathbf{Z}_p \longrightarrow \mathbf{Z}_p/p^m\mathbf{Z}_p.$$

Consider the corresponding semidirect product

$$G = B \rtimes \mathbf{Z}_p.$$

Then $cd_p(G) = p^m + 1$.

7.5 Groups G with $cd_p(G) \leq 1$

Let G be a profinite group. Recall (see Definition 3.5.1) that an embedding problem for G is a diagram of profinite groups and continuous homomorphisms

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \big\downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array} \tag{2}$$

with exact row, and where φ is an epimorphism.

Theorem 7.5.1 *Let G be a profinite group and p a prime number. The following statements are equivalent*:

(a) $cd_p(G) \leq 1$;

(b) *The embedding problem* (2) *is weakly solvable whenever A is finite and K is a finite elementary abelian p-group*;

(c) *Every short exact sequence of profinite groups*

$$1 \longrightarrow K \longrightarrow A \longrightarrow G \longrightarrow 1,$$

where K is a finite elementary abelian p-group, splits;

(d) *The embedding problem* (2) *is weakly solvable whenever K is a pro-p group*;

(e) *Every short exact sequence of profinite groups*

$$1 \longrightarrow K \longrightarrow A \longrightarrow G \longrightarrow 1,$$

where K is any pro-p-group, splits.

Proof. The implications (d) $\Rightarrow$ (e) $\Rightarrow$ (c) and (d) $\Rightarrow$ (b) are clear.

(b) $\Rightarrow$ (d): First, observe that if A is a profinite group and K is an abelian p-group which is a minimal normal subgroup of A, then K is annihilated by p. Hence (d) is equivalent (b) by Lemma 3.5.5.

(a) $\Rightarrow$ (b): We need a continuous homomorphism $\eta : G \longrightarrow A$ such that $\alpha\eta = \varphi$. Let $f : B \times B \longrightarrow K$ be a representative in $H^2(B, K)$ corresponding to the extension

$$1 \longrightarrow K \longrightarrow A \xrightarrow{\alpha} B \longrightarrow 1,$$

(see Theorem 6.8.4). We associate a cocycle $g : G \times G \longrightarrow K$ to f by defining

$$g(x, y) = f(\varphi(x), \varphi(y))$$

(i.e., $g = \mathrm{Inf}(f)$, where Inf is the inflation map). Note that there is an action of G on K induced by φ, namely, if $a \in K$ and $x \in G$, then $xa = \varphi(x)a$.

To g there corresponds an extension

$$1 \longrightarrow K \longrightarrow \bar{A} \xrightarrow{\bar{\alpha}} G \longrightarrow 1$$

which must split since by hypothesis $H^2(G, K)_p = 0$. Say $\sigma : G \longrightarrow \bar{A}$ is a continuous homomorphism with $\bar{\alpha}\sigma = \mathrm{id}_G$. We identify A and $\bar{A}$ with the direct products $K \times B$ and $K \times G$ respectively (see the proof of Theorem 6.8.4). Define

$$\gamma : \bar{A} \longrightarrow A$$

by $\gamma(a, x) = (a, \varphi(x))$ $(a \in K, x \in G)$. One easily checks that γ is a continuous homomorphism (see Theorem 6.8.4 for the definition of the operation in A and $\bar{A}$, and their topologies) making the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & K & \longrightarrow & \bar{A} & \underset{\sigma}{\overset{\bar{\alpha}}{\rightleftarrows}} & G & \longrightarrow & 1 \\
 & & \big\downarrow{\scriptstyle \mathrm{id}} & & \big\downarrow{\scriptstyle \gamma} & & \big\downarrow{\scriptstyle \varphi} & & \\
1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1
\end{array}$$

commutative.

Define $\eta : G \longrightarrow A$ by $\eta = \gamma\sigma$. Then $\alpha\eta = \varphi$, as desired.

(c) $\Rightarrow$ (a): According to (c), $H^2(G, K) = 0$, whenever K is a G-module which is an elementary abelian p-group. Now, every p-primary discrete simple $[\![\mathbf{Z}G]\!]$-module is a finite elementary abelian p-group; therefore $H^2(G, K) = 0$ for every p-primary discrete simple $[\![\mathbf{Z}G]\!]$-module K. Hence the result follows from Proposition 7.1.4. $\square$

Corollary 7.5.2 *Let F be a free pro-p group of rank at least* 1. *Then*

$$cd_p(F) = cd(F) = 1.$$

Proof. Since $F \neq 1$, $cd(F) \geq 1$. We shall prove that (e) of the theorem above holds. Let F be free on the set X converging to 1, and let $\iota : X \longrightarrow F$ be the canonical embedding. Let

$$1 \longrightarrow P \longrightarrow A \xrightarrow{\alpha} F \longrightarrow 1,$$

be an exact sequence, where P is a pro-p-group. Let $\sigma : F \longrightarrow A$ be a continuous section with $\sigma(1) = 1$ (see Proposition 2.2.2). Then the map $\sigma\iota : X \longrightarrow A$ converges to 1. Since P and F are pro-p-groups, so is A. Hence there is a continuous homomorphism $\psi : F \longrightarrow A$ with $\psi\iota = \sigma\iota$. Thus $\alpha\psi$ is the identity on F. This verifies (e) and so, by Theorem 7.5.1, $cd(F) \leq 1$. □

See Theorem 7.7.4 for a converse of the above corollary. The following result is obtained using a similar argument.

Corollary 7.5.3 *Let $\mathcal{C}$ be NE-formation of finite groups (see Section 2.1) and let F be a nontrivial free pro-$\mathcal{C}$ group. Then $cd_p(F) = 1$ for every prime p.*

Some parts of Theorem 7.5.1 can be sharpen in a certain direction. Recall that if π is a set of primes, a π-group is a profinite group whose order involves only primes in π.

Proposition 7.5.4 *Let G be a profinite group and let π be a fixed set of primes. The following conditions are equivalent*:

(a) $cd_p(G) \leq 1$ *for each* $p \in \pi$;
(b) *Every embedding problem* (2) *where A is finite and K is a π-group, is weakly solvable*;
(c) *Every embedding problem* (2), *where K is any profinite π-group, is weakly solvable.*

Proof. The equivalence of conditions (b) and (c) follows from Lemma 3.5.5. The implication (b) ⇒(a) is a consequence of Theorem 7.5.1. Here we prove that (a) implies (b). Consider an embedding problem (2) with A finite and K a π-group. We use induction on the order of K to show that the embedding problem (2) is weakly solvable. If $K = 1$, this is clear. Assume that $K \neq 1$ and, for a fixed $p \in \pi$, consider a p-Sylow subgroup P of K. We may assume $P \neq K$, for otherwise the embedding problem is solvable according to Theorem 7.5.1. We shall distinguish two cases:

(1) P is a normal subgroup of A. Then P is the unique p-Sylow subgroup of K, and hence normal in A. By the induction hypothesis, the embedding problem

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K/P & \longrightarrow & A/P & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array}$$

is weakly solvable. Say $\varphi_1 : G \longrightarrow A/P$ is a solution. Then, again by induction, the embedding problem

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \big\downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & P & \longrightarrow & A & \xrightarrow{\alpha} & A/P & \longrightarrow & 1 \end{array}$$

is weakly solvable. Hence the original embedding problem is solvable.

(2) P is not normal in A. By the Frattini argument (see Exercise 2.3.13), $A = KN$, where $N = N_A(P)$ is the normalizer of P in A. Note that $N \cap K < K$ since P is obviously not normal in K. Therefore, $\alpha(N) = \alpha(A) = B$. Then

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \big\downarrow{\scriptstyle \varphi_1} & & \\ 1 & \longrightarrow & K \cap N & \longrightarrow & N & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array}$$

is an embedding problem. This is weakly solvable by induction. Thus the original problem is weakly solvable since $N \leq A$. □

7.6 Projective Profinite Groups

Let $\mathcal{C}$ be a variety of finite groups. We say that a pro-$\mathcal{C}$ group is *$\mathcal{C}$-projective* if it is a projective object in the category of pro-$\mathcal{C}$ groups, i.e., if every embedding problem

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \big\downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array} \tag{3}$$

of pro-$\mathcal{C}$ groups is weakly solvable. A profinite group is called *projective* if it is $\mathcal{C}$-projective for the variety $\mathcal{C}$ of all finite groups.

As an immediate consequence of Lemma 3.5.5, we have

Lemma 7.6.1 *A pro-$\mathcal{C}$ group G is $\mathcal{C}$-projective if and only if every embedding problem (3) with $A \in \mathcal{C}$ is weakly solvable.*

Example 7.6.2 Let $\mathcal{C}$ be a variety of finite groups. Then every free pro-$\mathcal{C}$ group is $\mathcal{C}$-projective. Indeed, let $F = F(X)$ be a free pro-$\mathcal{C}$ group on a set X converging to 1 (recall that every free pro-$\mathcal{C}$ group is of this type: see Proposition 3.5.12). Consider an embedding problem for F

$$\begin{array}{ccccccccc} & & & & & & F & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \stackrel{\alpha}{\longrightarrow} & B & \longrightarrow & 1 \end{array}$$

Let $\sigma : B \longrightarrow A$ be a continuous section (see Proposition 2.2.2) for α. Let $\rho : X \longrightarrow A$ be the restriction of $\sigma\varphi$ to X. Since the restriction of φ to X converges to 1, so does ρ. Let $\bar\rho : F \longrightarrow A$ be the unique continuous homomorphism extending ρ. Then $\alpha\bar\rho = \varphi$, proving that the embedding problem above is weakly solvable.

When the variety $\mathcal{C}$ is extension closed (see Section 2.1), the following lemma provides a complete characterization of $\mathcal{C}$-projective groups in terms of free groups.

Lemma 7.6.3 *Let $\mathcal{C}$ be a variety of finite groups and let G be a pro-$\mathcal{C}$ group.*

(a) *If G is $\mathcal{C}$-projective, then it is isomorphic to a closed subgroup of a free pro-$\mathcal{C}$ group.*
(b) *Assume in addition that the variety $\mathcal{C}$ is extension closed (see Section 2.1). Then G is $\mathcal{C}$-projective if and only if G is a closed subgroup of a free pro-$\mathcal{C}$ group.*

Proof. (a) By Theorem 3.3.16, there exists a free pro-$\mathcal{C}$ group F and a continuous epimorphism $\alpha : F \longrightarrow G$. Since G is $\mathcal{C}$-projective, there exists a continuous homomorphism $\sigma : G \longrightarrow F$ such that $\alpha\sigma = \mathrm{id}_G$. Hence σ is an embedding.

(b) Assume that $G \le_c F$, where F is a free pro-$\mathcal{C}$ group. Consider an embedding problem (3) as above with $A \in \mathcal{C}$. Then $\mathrm{Ker}(\varphi)$ is an open normal subgroup of G. Hence there exists $V \triangleleft_o F$ such that $V \cap G \le \mathrm{Ker}(\varphi)$. Since GV is open in F and the variety $\mathcal{C}$ is extension closed, it follows that GV is a free pro-$\mathcal{C}$ group (see Theorem 3.6.2). Therefore we may assume that $F = GV$. Put $U = V\mathrm{Ker}(\varphi)$. Then $U \triangleleft_o F$ and $U \cap G = \mathrm{Ker}(\varphi)$. Define an epimorphism $\varphi_1 : F \longrightarrow B$ to be the composite of the natural maps

$$F \longrightarrow F/U = GU/U \longrightarrow G/G \cap U = G/\mathrm{Ker}(\varphi) \longrightarrow B.$$

Note that φ is the restriction of φ_1 to G. Since F is $\mathcal{C}$-projective, there exists a continuous homomorphism $\bar\varphi_1 : F \longrightarrow A$ such that $\alpha\bar\varphi_1 = \varphi_1$. Therefore, the restriction of $\bar\varphi_1$ to G is a weak solution of the embedding problem (3), as needed. □

Definition 7.6.4 *A variety of finite groups $\mathcal{C}$ is called 'saturated' if whenever G is a finite group and its Frattini quotient $G/\Phi(G)$ belongs to $\mathcal{C}$, then G is in $\mathcal{C}$.*

Example 7.6.5 The following are examples of saturated varieties of finite groups.

(1) Every extension closed variety. This follows from the fact that if G is a finite group and p is a prime number which divides the order of the Frattini subgroup $\Phi(G)$ of G, then p divides the order of the Frattini quotient $G/\Phi(G)$ (cf. Huppert [1967], Satz III.3.8). Since $\Phi(G)$ is nilpotent, this means that it is in $\mathcal{C}$. Therefore, $G \in \mathcal{C}$.
(2) The variety of all finite nilpotent groups (cf. Huppert [1967], Satz III.3.7).
(3) The variety of all finite supersolvable groups (cf. Huppert [1967], Satz VI.8.6).

Our interest in saturated varieties stems from the following result.

Lemma 7.6.6 *Let $\mathcal{C}$ be a saturated variety of finite groups. Let $\alpha : A \longrightarrow B$ be an epimorphism of finite groups with $B \in \mathcal{C}$. Then there exists a subgroup M of A such that $M \in \mathcal{C}$ and $\alpha(M) = B$.*

Proof. Let $N = \mathrm{Ker}(\alpha)$. Consider the set of all complements of N in A:

$$\mathcal{M} = \{H \mid H \leq A, NH = A.\}$$

Note that $\mathcal{M} \neq \emptyset$ since $A \in \mathcal{M}$. Let M be a minimal element of $\mathcal{M}$. It will suffice to show that $M \in \mathcal{C}$. In order to see this, we first show that $M \cap N \leq \Phi(M)$. Indeed, if $M \cap N \not\leq \Phi(M)$, then there is a maximal subgroup T of M such that $M \cap N \not\leq T$; hence $(M \cap N)T = M$. So $A = NM = NT$, contradicting the minimality of M. Thus we have shown that $M \cap N \leq \Phi(M)$. From $A = NM$, we deduce that

$$M/M \cap N \cong A/N \in \mathcal{C}.$$

Since $\mathcal{C}$ is closed under taking quotients, one has that $M/\Phi(M) \in \mathcal{C}$, and so $M \in \mathcal{C}$, because $\mathcal{C}$ is saturated. □

Proposition 7.6.7 *Let $\mathcal{C}$ be a saturated variety of finite groups and let G be a pro-$\mathcal{C}$ group. Then the following conditions on G are equivalent*:

(a) *G is a $\mathcal{C}$-projective group*;
(b) *G is a projective group*;
(c) *$cd(G) \leq 1$.*

Proof. Clearly (b) implies (a). The equivalence of (b) and (c) follows from Proposition 7.5.4. Hence it remains to prove that (a) implies (b). Consider an embedding problem for G

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array}$$

where K, A and B are arbitrary finite groups. Since φ is an epimorphism and G is a pro-$\mathcal{C}$ group, we have that $B \in \mathcal{C}$. By Lemma 7.6.6 there exists a subgroup M of A such that $M \in \mathcal{C}$ and $\alpha(M) = B$. Therefore by (a), there exists a continuous homomorphism $\bar{\varphi} : G \longrightarrow M \hookrightarrow A$ with $\alpha\bar{\varphi} = \varphi$. Thus (b) holds. □

Corollary 7.6.8 *Let $\mathcal{C}$ be a saturated variety of finite groups and let B be a pro-$\mathcal{C}$ group. Suppose that $\alpha : A \longrightarrow B$ is an epimorphism of profinite groups. Then A contains a closed pro-$\mathcal{C}$ subgroup H such that $\alpha(H) = B$.*

Proof. Let $\varphi : F \longrightarrow A$ be a continuous epimorphism, where F is a free pro-$\mathcal{C}$ group (see Theorem 3.3.16). As mentioned in Example 7.6.5, the group F is $\mathcal{C}$-projective. By Proposition 7.6.7, we deduce that F is projective. Hence there exists a homomorphism $\bar{\varphi} : F \longrightarrow A$ with $\alpha\bar{\varphi} = \varphi$. Then take $H = \mathrm{Im}(\bar{\varphi})$. □

Proposition 7.6.9 *Let $\mathcal{C}$ be a variety of finite groups and let G and H be pro-$\mathcal{C}$ groups.*

(a) *Assume G is $\mathcal{C}$-projective. Then every continuous epimorphism*

$$\rho : G/\Phi(G) \longrightarrow H/\Phi(H)$$

of Frattini quotients can be lifted to a continuous epimorphism

$$\psi : G \longrightarrow H,$$

i.e., the following diagram commutes

$$\begin{array}{ccc} G & \xrightarrow{\ \psi\ } & H \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ G/\Phi(G) & \xrightarrow{\ \rho\ } & H/\Phi(H), \end{array}$$

where α and β are the canonical epimorphisms.

(b) *Assume that both G and H are $\mathcal{C}$-projective. Then every continuous isomorphism $\rho : G/\Phi(G) \longrightarrow H/\Phi(H)$ can be lifted to a continuous isomorphism $\psi : G \longrightarrow H$.*

Proof. (a) Since G is $\mathcal{C}$-projective, there exists a continuous homomorphism $\psi : G \longrightarrow H$ lifting ρ. Hence $\psi(G)\Phi(H) = H$. Thus $\psi(G) = H$ (see Corollary 2.8.5).

(b) By part (a), there exists a continuous epimorphism $\psi : G \longrightarrow H$ such that $\beta\psi = \rho\alpha$. Since ρ is an injection, $\mathrm{Ker}(\psi) \le \Phi(G)$. Since H is $\mathcal{C}$-projective, there exists a continuous homomorphism $\xi : H \longrightarrow G$ such that $\psi\xi = \mathrm{id}_H$. So ξ is a injection and, in addition, $\xi(H)\mathrm{Ker}(\psi) = G$. Therefore, $\xi(H) = G$ (see Corollary 2.8.5). Thus, ξ is an isomorphism. Consequently, ψ is an isomorphism. □

Corollary 7.6.10 *Let F be a pro-p group. Let $y_1, \dots, y_n \in F$ be linearly independent mod $\Phi(F)$. Then there exists a basis Y of F converging to 1 containing the elements $y_1, \dots, y_n$.*

Proof. Let $\pi : F \longrightarrow F/\Phi(F)$ be the canonical epimorphism. We think of $F/\Phi(F)$ as a free pro-$\mathcal{C}$ group, where $\mathcal{C}$ is the class of all finite elementary abelian p-groups. Choose a basis $\bar{Y}$ converging to 1 of $F/\Phi(F)$ such that $\pi(y_i) \in \bar{Y}$ $(i = 1, \dots, n)$ and such that $\operatorname{rank}(F) = |\bar{Y}|$ (this can be done as follows: consider the finite subgroup A of $F/\Phi(F)$ generated by $\pi(y_1), \dots, \pi(y_n)$; by Proposition 2.8.16, $F/\Phi(F) = A \oplus B$ for some closed subgroup B of $F/\Phi(F)$; it is easy to see that in this case, B is a free pro-$\mathcal{C}$ group; then $\bar{Y}$ can be taken to be the union of $\pi(y_1), \dots, \pi(y_n)$ and a basis converging to 1 of the free pro-$\mathcal{C}$ group B).

Let X be a basis of F converging to 1. Then

$$\bar{X} = \{\bar{x} = \pi(x) \mid x \in X\}$$

is a basis of $F/\Phi(F)$ converging to 1. Consider a bijection $\varphi : \bar{X} \longrightarrow \bar{Y}$. Choose a continuous homomorphism $\bar{\varphi} : F \longrightarrow F$ lifting φ such that $\bar{\varphi}(x_i) = y_i$ $(i = 1, \dots, n)$. By Proposition 7.6.9, $\bar{\varphi}$ is an isomorphism. Therefore, $Y = \bar{\varphi}(X)$ is the basis we were seeking. □

Exercise 7.6.11 Let $\mathcal{C}$ be a variety of finite groups and let $\{G_i, \varphi_{ij}, I\}$ be an inverse system of $\mathcal{C}$-projective pro-$\mathcal{C}$ groups over a poset I. Prove that

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

is $\mathcal{C}$-projective. (Hint: use Lemma 1.1.16.)

7.7 Free Pro-p Groups and Cohomological Dimension

In this section we show that projective pro-p groups are precisely free pro-p groups.

If G is a pro-p group, we denote by $H^n(G)$ the cohomology group $H^n(G, \mathbf{Z}/p\mathbf{Z})$. Recall that the Frattini subgroup of G is $\Phi(G) = \overline{[G,G]G^p}$ (see Lemma 2.8.7).

Remark 7.7.1

(a) Let G be a pro-p group. Then

$$H^1(G) \cong \bigoplus_X \mathbf{Z}/p\mathbf{Z},$$

the direct sum of $|X|$ copies of $\mathbf{Z}/p\mathbf{Z}$, for some indexing set X. This is clear since $H^1(G) = \operatorname{Hom}(G/\Phi(G), \mathbf{Z}/p\mathbf{Z})$ is an elementary abelian p-group.

(b) Let $F = F(X)$ be a free pro-p group on the set X converging to 1. Then

$$\begin{aligned} H^1(F) = \operatorname{Hom}(F, \mathbf{Z}/p\mathbf{Z}) &\cong \{h : X \longrightarrow \mathbf{Z}/p\mathbf{Z} \mid h \text{ converges to } 0\} \\ &\cong \bigoplus_X \mathbf{Z}/p\mathbf{Z}. \end{aligned}$$

(c) Let G be a pro-p group. Then, $H^1(G)$ and $G/\Phi(G)$ are Pontryagin dual, where $\Phi(G)$ is the Frattini subgroup of G. Indeed,

$$\begin{aligned}\mathrm{Hom}(G/\Phi(G), \mathbf{Q}/\mathbf{Z}) &\cong \mathrm{Hom}(G/\Phi(G), \mathbf{Z}/p\mathbf{Z})\\ &\cong \mathrm{Hom}(G, \mathbf{Z}/p\mathbf{Z}) = H^1(G).\end{aligned}$$

(d) Let G_1 and G_2 be pro-p groups and let

$$\psi : G_1 \longrightarrow G_2$$

be a continuous homorphism. Then ψ induces a homomorphism

$$H^1(\psi) : H^1(G_2) = \mathrm{Hom}(G_2, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^1(G_1) = \mathrm{Hom}(G_1, \mathbf{Z}/p\mathbf{Z})$$

given by

$$f \mapsto f\psi \quad (f \in \mathrm{Hom}(G_2, \mathbf{Z}/p\mathbf{Z})).$$

The map ψ also induces a homomorphism of Frattini quotient groups

$$\rho : G_1/\Phi(G_1) \longrightarrow G_2/\Phi(G_2)$$

since $\psi(G_1) \leq G_2$. Note that ρ and $H^1(\psi)$ are Pontryagin dual to each other.

Proposition 7.7.2 *Let $\psi : G_1 \longrightarrow G_2$ be a continuous homomorphism of pro-p groups. Then the following statements are equivalent.*

(a) *ψ is surjective*;
(b) *$H^1(\psi) : H^1(G_2) \longrightarrow H^1(G_1)$ is injective*;
(c) *$\rho : G_1/\Phi(G_1) \longrightarrow G_2/\Phi(G_2)$ is surjective.*

Proof. If ψ is surjective, it is obvious that $H^1(\psi)$ is injective. Conversely, assume that $H^1(\psi)$ is injective and that $\psi(G_1) \neq G_2$. Choose a maximal open subgroup U of G_2 containing $\psi(G_1)$. Since G_2 is a pro-p group, U is normal of index p (see Lemma 2.8.7). Then the canonical homomorphism

$$f : G_2 \longrightarrow G_2/U \cong \mathbf{Z}/p\mathbf{Z}$$

is non-trivial. However $H^1(\psi)(f) = f\psi = 0$. A contradiction. This proves the equivalence of (a) and (b).

The equivalence of (a) and (c) follows from Corollary 2.8.8 and Proposition 7.6.9. □

Lemma 7.7.3 *Let G_1 and G_2 be pro-p groups and assume that $cd_p(G_1) \leq 1$. Then every homomorphism $\alpha : H^1(G_2) \longrightarrow H^1(G_1)$ is of the form $H^1(\psi)$, for some continuous homomorphism $\psi : G_1 \longrightarrow G_2$.*

Proof. Let $\rho : G_1/\Phi(G_1) \longrightarrow G_2/\Phi(G_2)$ be the dual map of α. It suffices to prove the existence of a continuous homomorphism $\psi : G_1 \longrightarrow G_2$ which induces ρ on the Frattini quotients (see Remark 7.7.1(d)). Consider the embedding problem

$$\begin{array}{ccc} & & G_1 \\ & & \downarrow \\ & & G_1/\Phi(G_1) \\ & & \downarrow \rho \\ G_2 & \longrightarrow & G_2/\Phi(G_2). \end{array}$$

Since $cd_p(G_1) \leq 1$, this embedding problem has a weak solution $\psi : G_1 \longrightarrow G_2$ (see Theorem 7.5.1). Clearly ψ induces the map ρ on the Frattini quotients. □

Theorem 7.7.4 *Let G be a pro-p group. Then, the following statements are equivalent*

(a) $cd_p(G) \leq 1$;
(b) $H^2(G) = 0$;
(c) *G is a free pro-p group*;
(d) *G is a projective group.*

Proof. By Corollary 7.1.6 and Proposition 7.6.7, the statements (a), (b) and (d) are equivalent. By Corollary 7.5.3, (c) implies (a). Conversely, assume that $cd_p(G) \leq 1$. According to Remark 7.7.1,

$$H^1(G) \cong \bigoplus_X \mathbf{Z}/p\mathbf{Z}$$

for some index set X. Consider a free pro-p group $F = F(X)$ on the set X converging to 1. Then (see Remark 7.7.1), there exists an isomorphism

$$\alpha : H^1(G) \longrightarrow H^1(F).$$

Therefore, its dual $\rho : F/\Phi(F) \longrightarrow G/\Phi(G)$ is an isomorphism. By Lemma 7.7.3, there is a continuous homomorphism $\psi : F \longrightarrow G$ such that $H^1(\psi) = \alpha$. By Propositions 7.7.2 and 7.6.9, ψ is an isomorphism. □

Corollary 7.7.5 *Every closed subgroup H of a free pro-p group G is a free pro-p group.*

Proof. By Theorem 7.3.1, $cd(H) \leq cd(G) \leq 1$. So the result follows from the theorem above. □

Corollary 7.7.6 *Let G be a profinite group. Then G is projective if and only if for any prime p, a p-Sylow subgroup G_p of G is a free pro-p group. In particular, a projective profinite group is torsion-free.*

The following corollary sharpens the content of Proposition 3.4.2.

Proposition 7.7.7 *Let G be a projective profinite group. Then, for every prime number p, its maximal pro-p quotient $G/R_p(G)$ is a free pro-p group.*

Proof. By Theorem 7.7.4, it suffices to show that $G/R_p(G)$ is projective. Consider the diagram

$$\begin{array}{ccccc} & & G & & \\ & & \big\downarrow{\scriptstyle \varphi_1} & & \\ & & G/R_p(G) & & \\ & & \big\downarrow{\scriptstyle \varphi} & & \\ A & \xrightarrow{\ \alpha\ } & B & \longrightarrow & 1 \end{array}$$

where α and φ are continuous epimorphisms of pro-p groups and where φ_1 is the canonical quotient map. We have to show that there is a continuous homomorphism $\bar{\varphi} : G/R_p(G) \longrightarrow A$ such that $\bar{\varphi}\alpha = \varphi$. Since G is projective, there exists a continuous homomorphism $\psi : G \longrightarrow A$ such that $\alpha\psi = \varphi\varphi_1$. Since $G/\mathrm{Ker}(\psi)$ is a pro-p group, we have $R_p(G) \le \mathrm{Ker}(\psi)$. Hence ψ factors through $G/R_p(G)$, i.e., there exists a homomorphism $\psi_1 : G/R_p(G) \longrightarrow A$ such that $\psi = \psi_1\varphi_1$. Define $\bar{\varphi}$ to be ψ_1. □

Exercise 7.7.8

(a) (Zassenhaus groups) Let G be a profinite group all whose Sylow subgroups are procyclic. Prove that G contains procyclic subgroups K and H of relatively prime orders such that K is normal in G and $G = K \rtimes H$. (Hint: for the corresponding property for finite groups, see Hall [1959], Theorem 9.4.3.)

(b) (Projective solvable groups) Let G be a solvable profinite group. Prove that if G is projective then there exists disjoint sets of primes σ and τ such that
$$G \cong \widehat{\mathbf{Z}}_\sigma \rtimes \widehat{\mathbf{Z}}_\tau.$$

7.8 Generators and Relators for Pro-p Groups

We recall that if G is a profinite group, $d(G)$ denotes the minimal cardinality of a set of generators of G converging to 1 (see Definition 2.4.5). If G is pro-p, then $H^n(G) = H^n(G, \mathbf{Z}/p\mathbf{Z})$ is in a natural way a vector space over the field $\mathbf{F}_p$ with p elements. In the sequel we write $\dim H^n(G)$ for $\dim_{\mathbf{F}_p} H^n(G)$, the dimension of $H^n(G)$ over $\mathbf{F}_p$.

Theorem 7.8.1 *Let G be a pro-p group. Then $d(G) = \dim H^1(G)$.*

Proof. Assume $\dim H^1(G) = |X|$, for some set X. Let $F = F(X)$ be a free pro-p group on the set X converging to 1. By Remark 7.7.1(b), $\dim H^1(F) = |X|$. Let

$$\alpha : H^1(G) \longrightarrow H^1(F)$$

be an isomorphism. It follows from Lemma 7.7.3 and Proposition 7.7.2 that there exists a surjective continuous homomorphism $\psi : F \longrightarrow G$. Thus

$$d(G) \leq |X| = \dim H^1(G).$$

Now, assume $d(G) = |Y|$, for some set Y. Let $F(Y)$ be a free pro-p group on the set Y converging to 1. Then there is a continuous epimorphism $\varphi : F(Y) \longrightarrow G$. By Proposition 7.7.2, φ induces an injection

$$H^1(G) \longrightarrow H^1(F(Y)).$$

Thus,

$$\dim H^1(G) \leq \dim H^1(F(Y)) = |Y| = d(G).$$ □

Let F be a free profinite group and let K be a closed normal subgroup of F. We say that a subset $R = \{r_i \mid i \in I\}$ of K converging to 1 is a *set of generators of K as a normal subgroup of F*, if the F-conjugates of the r_i generate algebraicly a dense subgroup of K, i.e., if K is the smallest closed normal subgroup of F containing the r_i. We define $d_F(K)$ to be the smallest cardinal of a generating set of K as a normal subgroup of F.

Proposition 7.8.2 *Let F be a pro-p group and let K be a closed normal subgroup of F. Then*

$$d_F(K) = \dim H^1(K)^F$$

where $H^1(K)^F$ is the fixed submodule of $H^1(K)$ under the action of F described in Remark 7.2.2.

Proof. First we show that $d_F(K) \geq \dim H^1(K)^F$. Assume $d_F(K) = |I|$, where $\{r_i \mid i \in I\}$ converges to 1 and generates K as a normal subgroup of F. Define a homomorphism

$$\alpha : H^1(K)^F \longrightarrow \bigoplus_I \mathbf{Z}/p\mathbf{Z}$$

by $\alpha(f)(i) = f(r_i)$ ($f \in H^1(K)^F = \mathrm{Hom}(K, \mathbf{Z}/p\mathbf{Z})^F$). Then α is an injection. Indeed, suppose $\alpha(f) = 0$. Then $f(r_i) = 0$ for all $i \in I$. Now, according to the definition of the action of F on $\mathrm{Hom}(K, \mathbf{Z}/p\mathbf{Z})$ (see Remark 7.2.2), we have that for $x \in F$,

$$f(xr_ix^{-1}) = (xf)(r_i) = xf(r_i) = 0.$$

So $f = 0$ on the dense subgroup $\langle xr_ix^{-1} \mid i \in I, x \in F\rangle$ of K. Thus $f = 0$.

Next we prove that $d_F(K) \leq \dim H^1(K)^F$. Observe that since $H^1(K)$ and $K/\Phi(K)$ are Pontryagin dual (see Remark 7.7.1), the inclusion map $H^1(K)^F \hookrightarrow H^1(K)$ induces a dual epimorphism $K/\Phi(K) \longrightarrow \tilde{K}$, where $\tilde{K}$ is the dual of $H^1(K)^F$. Put

$$H^1(K)^F = \bigoplus_J (\mathbf{Z}/p\mathbf{Z}) f_j,$$

where $\{f_j : K \longrightarrow \mathbf{Z}/p\mathbf{Z} \mid j \in J\}$ is a basis for $H^1(K)^F$. Hence,

$$\tilde{K} \cong \prod_{j \in J} (\mathbf{Z}/p\mathbf{Z}) x_j$$

where $f_j(x_i) = 0$ or 1, according to whether $j = i$ or $j \neq i$. Let $F(J)$ be the free pro-p group on the set J converging to 1, and consider the diagram

$$\begin{array}{ccc} & & K \\ & & \downarrow \\ & & K/\Phi(K) \\ & & \downarrow \\ F(J) & \xrightarrow{\varphi} & \tilde{K} \end{array}$$

where the continuous homomorphism φ is defined by $\varphi(j) = x_j$ $(j \in J)$. Since $F(J)$ is projective, φ can be lifted to a continuous homomorphism $\bar{\varphi} : F(J) \longrightarrow K$. Set $v_j = \bar{\varphi}(j)$ $(j \in J)$. Then $\{v_j \mid j \in J\}$ is a subset of K converging to 1.

To prove that $d_F(K) \leq \dim H^1(K)^F$, it suffices to establish the following *Claim*: $\{v_j \mid j \in J\}$ is a set of generators of K as a normal subgroup of F. To prove this claim, let K' be the smallest closed normal subgroup of F containing the v_j. Then $K' \hookrightarrow K$. We shall show that this map is surjective, or equivalently, that its dual map

$$\alpha : H^1(K) \longrightarrow H^1(K')$$

is an injection. First we prove that its restriction

$$\bar{\alpha} : H^1(K)^F \longrightarrow H^1(K')^F$$

is an injection: let $f \in H^1(K)^F$, and assume that $f(K') = 0$. Then $f(v_j) = 0$; so $f(x_j) = 0$ for all $j \in J$. Hence $f(\tilde{K}) = 0$. Therefore, $f = 0$.

Finally we show that this implies that α is an injection. Indeed, since $\bar{\alpha}$ an injection, $\mathrm{Ker}(\alpha)$ contains no element different from 0 which is invariant under F. If $\mathrm{Ker}(\alpha) \neq 0$, it would contain a simple F-submodule all whose elements are fixed by F (see Lemma 7.1.5), a contradiction. Thus the claim is proved. □

Let G be a pro-p group and let $\{x_i \mid i \in I\}$ be a set of generators of G converging to 1. Let $F = F(I)$ be a free pro-p group on the set I converging to 1. Then there exists a unique continuous epimorphism

$$\varphi : F \longrightarrow G$$

mapping i to x_i ($i \in I$). Let K be its kernel. A set R of generators of K (as a normal subgroup of F) is called a set of *defining relators* corresponding to the set of generators $\{x_i \mid i \in I\}$.

We then say that

$$\langle x_1, \dots, x_n \mid R\rangle$$

is a *presentation* of G as a pro-p group. (One can give an analogous definition of 'presentation' for a general profinite group, using a free profinite group instead: see Appendix C.)

Assume now that $d(G) = |I| = d$ is finite and let F and K be as above. Then, define

$$rr(G) = \textit{relation rank}\,(G) = d_F(K).$$

The next result shows that $rr(G)$ is independent of the choice of the minimal set of generators $\{x_1, \dots, x_d\}$ of G.

Theorem 7.8.3 *Let G be a finitely generated pro-p group. Then*

$$rr(G) = \dim H^2(G).$$

Proof. Let $d(G) = |I| = d$, and consider the exact sequence described above

$$1 \longrightarrow K \longrightarrow F \longrightarrow G \longrightarrow 1,$$

where $F = F(I)$ is a free pro-p group on the finite set I. By Corollary 7.2.5, we obtain a five term exact sequence

$$0 \longrightarrow H^1(G) \longrightarrow H^1(F) \longrightarrow H^1(K)^F \longrightarrow H^2(G) \longrightarrow H^2(F).$$

Since both $H^1(G)$ and $H^1(F)$ are finite dimensional $\mathbf{F}_p$-vector spaces of the same dimension (see Theorem 7.8.1), the monomorphism

$$H^1(G) \longrightarrow H^1(F)$$

is an isomorphism. Since F is free pro-p, we have $H^2(F) = 0$. Hence $H^1(K)^F \cong H^2(G)$. Therefore, the result follows from Proposition 7.8.2. □

Now, let G be a finite p-group. Then $d(G) = \dim H^1(G)$ and $rr(G) = \dim H^2(G)$. Clearly, both $d(G)$ and $rr(G)$ are finite, since in this case the kernel K is finitely generated as a profinite group.

Proposition 7.8.4 *Let G be a finite p-group. Then*

$$rr(G) - d(G) = d(H^3(G, \mathbf{Z})).$$

Proof. Consider the short exact sequence

$$0 \longrightarrow \mathbf{Z} \xrightarrow{p} \mathbf{Z} \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow 0,$$

where p indicates multiplication by p. From this we obtain a corresponding exact sequence in cohomology

$$0 \longrightarrow H^1(G) \longrightarrow H^2(G,\mathbf{Z}) \xrightarrow{p} H^2(G,\mathbf{Z}) \longrightarrow H^2(G) \longrightarrow H^3(G,\mathbf{Z})[p] \longrightarrow 0,$$

where $H^3(G,\mathbf{Z})[p]$ denotes the subgroup of elements of $H^3(G,\mathbf{Z})$ annihilated by p. Since G is finite, each $H^i(G,\mathbf{Z})$ $(i \geq 1)$ is a finitely generated abelian torsion group, and hence finite. Therefore,

$$\dim H^1(G) - \dim H^2(G,\mathbf{Z}) + \dim H^2(G,\mathbf{Z}) - \dim H^2(G) + \dim H^3(G,\mathbf{Z})[p] = 0.$$

Thus,

$$rr(G) - d(G) = \dim H^3(G,\mathbf{Z})[p].$$

On the other hand it is plain that $\dim H^3(G,\mathbf{Z})[p] = d(H^3(G,\mathbf{Z}))$, since $H^3(G,\mathbf{Z})$ is a finite abelian p-group. □

We mention the following result without proof (see Section 7.10 for references).

Theorem 7.8.5 (The Golod-Shafarevich inequality) *Let G be a nontrivial finite p-group. Then*

$$rr(G) > (d(G))^2/4.$$

7.9 Cup Products

Let G be a profinite group and let $A, B \in \mathbf{DMod}(G)$. Consider the tensor product over the ring of integers $A \otimes_{\mathbf{Z}} B$. In this section we shall write $A \otimes B$ instead of $A \otimes_{\mathbf{Z}} B$. Define an action of G on $A \otimes_{\mathbf{Z}} B$ by $x(a \otimes b) = xa \otimes xb$ $(x \in G, a \in A, b \in B)$. Under this action $A \otimes B$ becomes a discrete G-module, since

$$A \otimes B = \bigcup_U (A \otimes B)^U,$$

where U runs through the set of all open subgroups of G.

Theorem 7.9.1 *Let G be a profinite group. Then there is a unique family of* $\mathbf{Z}$*-linear maps, called 'cup products',*

$$H^n(G,A) \times H^m(G,B) \to H^{n+m}(G, A \otimes B),$$

denoted $(a,b) \mapsto a \cup b$, defined for every pair n, m of natural numbers and every pair of discrete G-modules A, B such that the following properties hold:

(a) *These maps are morphisms of functors when we consider each side as a covariant bifunctor on* (A, B);

(b) *For* $n = m = 0$, *the map*

$$H^0(G, A) \times H^0(G, B) = A^G \times B^G \longrightarrow H^0(G, A \otimes B) = (A \otimes B)^G$$

is given by $(a, b) \mapsto a \otimes b$;

(c) *Let* $B \in \mathbf{DMod}(G)$. *If*

$$0 \longrightarrow A \longrightarrow A' \longrightarrow A'' \longrightarrow 0$$

is an exact sequence in $\mathbf{DMod}(G)$ *and if*

$$0 \longrightarrow A \otimes B \longrightarrow A' \otimes B \longrightarrow A'' \otimes B \longrightarrow 0$$

is also exact, then the diagram

$$\begin{array}{ccc} H^n(G, A'') \times H^m(G, B) & \xrightarrow{\delta \times \mathrm{id}} & H^{n+1}(G, A) \times H^m(G, B) \\ \downarrow \cup & & \downarrow \cup \\ H^{n+m}(G, A'' \otimes B) & \xrightarrow{\delta} & H^{n+m+1}(G, A \otimes B) \end{array}$$

commutes, where δ *denotes the connecting homomorphism corresponding to the above exact sequences; in other words, if* $a'' \in H^n(G, A'')$ *and* $b \in H^m(G, B)$ *then*

$$\delta(a'' \cup b) = \delta(a'') \cup b;$$

(d) *Let* $A \in \mathbf{DMod}(G)$. *If*

$$0 \longrightarrow B \longrightarrow B' \longrightarrow B'' \longrightarrow 0$$

is an exact sequence in $\mathbf{DMod}(G)$ *and if*

$$0 \longrightarrow A \otimes B \longrightarrow A \otimes B' \longrightarrow A \otimes B'' \longrightarrow 0$$

is also exact, then the diagram

$$\begin{array}{ccc} H^n(G, A) \times H^m(G, B'') & \xrightarrow{\mathrm{id} \times \delta} & H^n(G, A) \times H^{m+1}(G, B) \\ \downarrow \cup & & \downarrow \cup \\ H^{n+m}(G, A \otimes B'') & \xrightarrow{(-1)^n \delta} & H^{n+m+1}(G, A \otimes B) \end{array}$$

commutes; that is, if $a \in H^n(G, A)$ *and* $b'' \in H^m(G, B'')$, *then*

$$(-1)^n \delta(a \cup b'') = a \cup \delta(b'').$$

Proof. Uniqueness: Let $A \in \mathbf{DMod}(G)$, and consider the exact sequence

$$0 \longrightarrow A \xrightarrow{\iota} C(G,A) \longrightarrow A'' \longrightarrow 0 \tag{4}$$

where $C(G,A)$ is the group of all continuous functions from G to A considered as a G-module (see Section 6.10), and ι is the G-homomorphism given by $\iota(a)(x) = xa$ $(x \in G, a \in A)$. Consider the map the map

$$\mu : C(G,A) \longrightarrow A$$

defined by $\mu(f) = f(1)$. Then μ is an abelian group homomorphism such that $\mu\iota =$ identity. Therefore, (4) splits as a sequence of abelian groups. Hence,

$$0 \longrightarrow A \otimes B \longrightarrow C(G,A) \otimes B \longrightarrow A'' \otimes B \longrightarrow 0$$

is an exact sequence of G-modules for every $B \in \mathbf{DMod}(G)$. On the other hand, by Corollary 6.10.6, $H^n(G, C(G,A)) = 0$ if $n \geq 1$. Hence, by property (c) we obtain a commutative diagram with exact upper row

$$\begin{array}{ccccc} H^n(A'') \times H^m(B) & \xrightarrow{\delta \times \mathrm{id}} & H^{n+1}(A) \times H^m(B) & \longrightarrow & 0 \times H^m(B) \\ \downarrow \cup & & \downarrow \cup & & \\ H^{n+m}(A'' \otimes B) & \xrightarrow{\delta} & H^{n+m+1}(A \otimes B) & & \end{array}$$

for $n, m \geq 0$ (in this diagram $H^r(X)$ stands for $H^r(G,X)$). By an induction argument, it follows that

$$H^0(G,A'') \times H^0(G,B) \longrightarrow H^0(G, A'' \otimes B)$$

uniquely determines the cup products

$$H^n(G,A) \times H^0(G,B) \longrightarrow H^n(G, A \otimes B) \quad (n \geq 0).$$

Using property (c) one sees in a similar way that these maps in turn determine uniquely the cup products

$$H^n(G,A) \times H^m(G,B) \longrightarrow H^m(G, A \otimes B).$$

Existence: To prove the existence of cup products we define first analogous maps at the level of the groups $C^n(G,-)$ of cochains (see Section 6.4). Given $n, m \geq 0$ and $A, B \in \mathbf{DMod}(G)$, we define a mapping

$$\psi_{n,m} : C^n(G,A) \times C^m(G,B) \longrightarrow C^{n+m}(G, A \otimes B),$$

by

$$\psi_{n,m}(a,b)(x_0, \ldots, x_{n+m}) = a(x_0, \ldots, x_n) \otimes b(x_n, \ldots, x_{n+m})$$

$(a \in C^n(G, A), b \in C^m(G, B))$. It is easy to see that

$$\psi_{n,m}(a, b) \in C^{n+m}(G, A \otimes B),$$

and that each $\psi_{n,m}$ is a homomorphism of abelian group on each variable.

One checks without difficulty that

$$\partial(\psi_{n,m}(a, b)) = \psi_{n+1,m}(\partial(a), b) + (-1)^n \psi_{n,m+1}(a, \partial(b))$$

for $a \in C^n(G, A)$ and $b \in C^m(G, B)$. From these formulas one deduces that the maps $\psi_{n,m}$ induce well-defined maps

$$\cup : H^n(G, A) \times H^m(G, B) \longrightarrow H^{n+m}(G, A \otimes B)$$

given by

$$a \cup b = \psi_{n,m}(a, b)$$

for $a \in H^n(G, A)$ and $b \in H^m(G, B)$ (by abuse of notation, we let a, b stand both for cocycles and the corresponding elements in the cohomology groups).

Finally we prove that the products $(a, b) \mapsto a \cup b$ satisfy the conditions of the theorem. Property (b) follows immediately from the definitions.

Property (a): Let $\alpha : A \longrightarrow A'$ and $\beta : B \longrightarrow B'$ be homomorphisms of discrete G-modules. Then the diagram

$$\begin{array}{ccc} H^n(G, A) \times H^m(G, B) & \xrightarrow{\cup} & H^{n+m}(G, A \otimes B) \\ \downarrow{\scriptstyle \tilde{\alpha} \times \tilde{\beta}} & & \downarrow{\scriptstyle \widetilde{\alpha \otimes \beta}} \\ H^n(G, A') \times H^m(G, B') & \xrightarrow{\cup} & H^{n+m}(G, A' \otimes B') \end{array}$$

commutes, where $\tilde{\alpha}, \tilde{\beta}, \widetilde{\alpha \otimes \beta}$ are the maps induced on the cohomology groups by α, β, $\alpha \otimes \beta$, respectively. Indeed,

$$\begin{aligned} &(\tilde{\alpha}(a) \cup \tilde{\beta}(b))(x_0, \ldots, x_{n+m}) \\ &\quad = \psi(\tilde{\alpha}(a), \tilde{\beta}(b))(x_0, \ldots, x_{n+m}) = \tilde{\alpha}(a)(x_0, \ldots, x_n) \otimes \tilde{\beta}(b)(x_n, \ldots, x_{n+m}) \\ &\quad = (\widetilde{\alpha \otimes \beta}(a \cup b))(x_0, \ldots, x_{n+m}) \end{aligned}$$

$(a \in H^n(G, A), b \in H^m(G, B))$.

Property (c): Let $B \in \mathbf{DMod}(G)$ and let

$$0 \longrightarrow A \xrightarrow{\alpha} A' \xrightarrow{\beta} A'' \longrightarrow 0$$

be an exact sequence in $\mathbf{DMod}(G)$ such that

$$0 \longrightarrow A \otimes B \xrightarrow{\alpha \otimes 1} A' \otimes B \xrightarrow{\beta \otimes 1} A'' \otimes B \longrightarrow 0$$

is also exact.

Next we recall the definition of the connecting homomorphism δ. Let $a'' \in C^n(G, A'')$ with $\partial(a'') = 0$, so that a'' represents an element of $H^n(G, A'')$. Then, $\delta(a'')$ is defined as follows (see the proof of Lemma 6.6.1): let $a' \in C^n(G, A')$ with $\tilde{\beta}(a') = a''$, and let $a \in C^{n+1}(G, A)$ be such that $\tilde{\alpha}(a) = \partial(a')$ (a exists since $(\tilde{\beta}\partial)(a') = (\partial\tilde{\beta})(a') = 0$). Hence, $\partial(a) = 0$, so that a represents an element of $H^{n+1}(G, A)$. We set $\delta(a'') = a$.

Assume that $b \in \mathcal{C}^m(G, B)$. Then, using Property (a), we have

$$\widetilde{\beta \otimes 1}(a' \cup b) = a'' \cup b,$$
$$\widetilde{\alpha \otimes 1}(a \cup b) = \partial(a') \cup b.$$

Hence,

$$\partial(a'' \cup b) = 0 \quad \text{and} \quad \partial(a \cup b) = 0.$$

Therefore, $a'' \cup b$ and $a \cup b$ represent elements of the cohomology groups $H^{n+m}(G, A'' \otimes B)$ and $H^{n+m+1}(G, A \otimes B)$, respectively. Thus, from the explicit definition of the connecting homomorphism δ, we deduce that

$$\delta(a'' \cup b) = a \cup b = \delta(a'') \cup b$$

(notice that, in the above considerations, a'' and b stand both for cocycles and for the corresponding elements of the cohomology groups). The verification of Property (d) can be done in a similar manner. □

Next we establish some of the basic properties of cup products.

Proposition 7.9.2 *Let G be a profinite group. Let $A, B \in$ **DMod(G)** and let $a \in H^n(G, A)$ and $b \in H^n(G, B)$. Then*

$$a \cup b = (-1)^{mn} b \cup a,$$

where $A \otimes B$ and $B \otimes A$ are identified canonically.

Proof. This is plain if $n = m = 0$. We proceed by induction. Suppose the result holds for $n = n_0$ and $m = m_0$, and assume $a \in H^{n_0+1}(G, A)$ and $b \in H^{m_0}(G, B)$. As in the uniqueness proof of Theorem 7.9.1, we can construct a commutative diagram with exact upper row

$$\begin{array}{ccccc} H^{n_0}(A'') \times H^{m_0}(B) & \xrightarrow{\delta \times \mathrm{id}} & H^{n_0+1}(A) \times H^{m_0}(B) & \longrightarrow & 0 \times H^{m_0}(B) \\ \downarrow \cup & & \downarrow \cup & & \\ H^{n_0+m_0}(A'' \otimes B) & \xrightarrow{\delta} & H^{n_0+m_0+1}(A \otimes B) & & \end{array}$$

for $n_0, m_0 \geq 0$ (in this diagram $H^r(X)$ stands for $H^r(G, X)$).

Let $a'' \in H^{n_0}(G, A'')$ be such that $\delta(a'') = a$. Using Property (d) of Theorem 7.9.1 and induction, one has

$$a \cup b = \delta(a'' \cup b) = (-1)^{n_0 m_0} \delta(b \cup a'') = (-1)^{n_0 m_0}(-1)^{m_0} b \cup \delta(a'')$$
$$= (-1)^{(n_0+1)m_0} b \cup a.$$

One proves similarly that if the result holds for $n = n_0$ and $m = m_0$, then it holds for $n = n_0$ and $m = m_0 + 1$. □

Proposition 7.9.3 *Let G be a profinite group. Let $A, B, C \in$ **DMod**(G) and assume that $a \in H^n(G, A)$, $b \in H^m(G, B)$, $c \in H^r(G, C)$. Then*

$$(a \cup b) \cup c = a \cup (b \cup c),$$

after the canonical identification of $(A \otimes B) \otimes C$ and $A \otimes (B \otimes C)$.

Proof. This follows immediately from the definition of the cup product and cohomology groups by means of cochains (see the proof of "existence" in Theorem 7.9.1 and Section 6.6). □

We now turn to the study of the relationship between cup products and the special maps Res, Cor and Inf (see Section 6.7). The next two results follow immediately from the description of Res and Inf in terms of cochains (see Sections 6.7 and 6.5).

Proposition 7.9.4 *Let H be a closed subgroup of a profinite group G. Let $A, B \in$ **DMod**(G) and assume that $a \in H^n(G, A)$ and $b \in H^m(G, B)$. Then*

$$\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b),$$

where Res *is the restriction map.*

Proposition 7.9.5 *Let H be a closed normal subgroup of a profinite group G. Let $A, B \in$ **DMod**(G) and assume that $a \in H^n(G/H, A^H)$, $b \in H^m(G/H, B^H)$. Then*

$$\mathrm{Inf}(a \cup b) = \mathrm{Inf}(a) \cup \mathrm{Inf}(b),$$

where Inf *is the inflation map.*

Proposition 7.9.6 *Let G be a profinite group and let H be an open subgroup of G. Let $a \in H^n(G, A)$ and $b \in H^m(G, B)$, where $A, B \in$ **DMod**(G). Then*

$$\mathrm{Cor}\big(a \cup \mathrm{Res}(b)\big) = \mathrm{Cor}(a) \cup b.$$

Proof. Assume first that $n = m = 0$. Then $a \in A^H$ and $b \in B^G$. Let $x_1, \dots, x_t$ be a set of representatives of the left cosets of H in G. Then (see Section 6.7),

$$\begin{aligned}\operatorname{Cor}\big(a\cup\operatorname{Res}(b)\big)&=\sum_{i=1}^{t}x_i(a\cup b)=\sum_{i=1}^{t}x_ia\otimes x_ib=\sum_{i=1}^{t}x_ia\otimes b\\&=\left(\sum_{i=1}^{t}x_ia\right)\cup b=\operatorname{Cor}(a)\cup b.\end{aligned}$$

Now we proceed by induction. Assume the formula holds true for $n=n_0$ and $m=m_0$. Let $a\in H^{n_0+1}(G,A)$ and $b\in H^{m_0}(G,B)$. Consider the split exact sequence of abelian groups

$$0\longrightarrow A\stackrel{\iota}{\longrightarrow}C(G,A)\longrightarrow A''\longrightarrow 0$$

(see proof of uniqueness in Theorem 7.9.1). Since $H^n\big(H,C(G,A)\big)=0$, for $n\geq 1$, there is $a''\in H^{n_0}(H,A)$ with $\delta(a'')=a$, where δ is the connecting homomorphism corresponding to the above short exact sequence and the cohomological functor $\{H^n(H,-)\}_{n\geq 0}$. Since

$$0\longrightarrow A\otimes B\longrightarrow C(G,A)\otimes B\longrightarrow A''\otimes B\longrightarrow 0$$

is also exact, we can apply property (c) of Theorem 7.9.1. Hence, taking into account that Res and Cor commute with δ (see Section 6.7), we have by the induction hypothesis

$$\begin{aligned}\operatorname{Cor}(a\cup\operatorname{Res}(b))&=\operatorname{Cor}(\delta(a'')\cup\operatorname{Res}(b))=\operatorname{Cor}(\delta(a''\cup\operatorname{Res}(b)))\\&=\delta(\operatorname{Cor}(a''\cup\operatorname{Res}(b)))=\delta((\operatorname{Cor}(a'')\cup b))\\&=\delta(\operatorname{Cor}(a''))\cup b=\operatorname{Cor}(\delta(a''))\cup b=\operatorname{Cor}(a)\cup b.\end{aligned}$$

Similarly, using property (d) of Theorem 7.9.1, one proves that if the formula holds for $n=n_0$ and $m=m_0$, it also holds for $n=n_0$ and $m=m_0+1$. Thus, by induction, the formula is valid for all $n,m\geq 0$. □

Corollary 7.9.7 *Under the hypotheses of Proposition 7.9.6 we have*

$$\operatorname{Cor}(\operatorname{Res}(b)\cup a)=b\cup\operatorname{Cor}(a).$$

Proof.

$$\begin{aligned}\operatorname{Cor}\big(\operatorname{Res}(b)\cup a\big)&=\operatorname{Cor}\big((-1)^{nm}a\cup\operatorname{Res}(b)\big)=(-1)^{nm}\operatorname{Cor}(a)\cup b\\&=b\cup\operatorname{Cor}(a).\end{aligned}$$

□

7.10 Notes, Comments and Further Reading

Most of the results in Sections 7.1, 7.3, 7.4, 7.5, 7.7, 7.8 and 7.9 are due to J. Tate; we are influenced by the presentation of some of these results in Serre [1995], Lang [1966] and Ribes [1970]. Theorem 7.3.6 was proved by

Scheiderer [1994, 1996], while Theorem 7.3.7 is due to Serre [1965]; Haran [1990] gives a different proof of Theorem 7.3.7 based on a suggestion in Serre [1971]. Our presentation of the Lyndon-Hochschild-Serre spectral sequence follows (and improves) the presentation in Ribes [1970]. The useful five term exact sequences of Corollary 7.2.5 appear, for abstract groups, in Hochschild and Serre [1953]. Proposition 7.2.7 was proved by Neukirch [1971] for pro-p groups, and in the form presented here for prosolvable groups, by Ribes [1974]. In Weigel and Zalesskii [2004] they complement Proposition 7.4.2 and prove that, with the same notation, $cd_p(G) = cd_p(K) + vcd_p(G/K)$ if $cd_p(G) < \infty$ and $H^n(K, \mathbf{Z}_p/p\mathbf{Z})$ is finite, where $n = cd_p(K)$. In Cossey, Kegel and Kovács [1980], a proof of Corollary 7.7.5 is given with no reference to cohomology. For a treatment of number fields using group cohomology, see Neukirch, Schmidt and Wingberg [2008].

Projective profinite groups have been studied by Gruenberg [1967]. Proposition 7.6.9 is due to him. Lemma 7.6.6 is due to Huppert [1954] (the result is valid, more generally, for saturated formations of finite groups). Exercise 7.7.8 is mentioned in Herfort and Ribes [1989a]. For the relationship between local and absolute properties such as freeness and projectivity in profinite groups, see Pletch [1982].

Let G be a finite p-group with, say, $d = d(G)$. Then one can consider the relation rank of G as an abstract group: let $\Phi = \Phi(I)$ be an abstract free group on a basis I of cardinality d. Consider a short exact sequence of abstract groups

$$1 \longrightarrow R \longrightarrow \Phi \longrightarrow G \longrightarrow 1.$$

Define the abstract relation rank $arr(G)$ of G as the smallest cardinality of a set of generators of R as a normal subgroup of Φ. Clearly $rr(G) \leq arr(G)$. Serre mentions (skeptically) the following question (cf. Serre [1995], page 32).

Open Question 7.10.1 *For what finite p-groups G does one have $rr(G) = arr(G)$?*

Theorem 7.8.5 was proved in a slightly weaker form by Golod and Shafarevich [1964]: what they actually proved was that $rr(G) > (d(G) - 1)^2/4$. The improvement is due to Gaschütz and to Vinberg, independently (cf. Roquette [1967]). Another proof of this inequality can be found in Serre [1995], Ch. I, Annex 3. Lubotzky [1983] studies pro-p groups satisfying the analog of the Golod-Shafarevich inequality and applications to abstract infinite groups. He shows that p-adic analytic groups satisfy the analogous inequality. As a consequence he proves the following

Theorem 7.10.2 *Let Γ be a finitely generated nilpotent group different from $\mathbf{Z}$, and let $\Gamma = \langle X \mid R \rangle$ be a minimal presentation of Γ. Then $|R| \geq |X|^2/4$.*

Answering a conjecture of J. Wilson, Zel'manov [2000] has proved the following

Theorem 7.10.3 *Let G be a finitely generated pro-p group satisfying the analog of Golod-Shafarevich's inequality. Then G contains a closed nonabelian free pro-p subgroup.*

Pro-p Groups G with one Defining Relator

A finitely generated pro-p group G is said to admit a presentation with a single defining relator if G has a presentation (as a pro-p group) of the form $G = \langle x_1, \ldots, x_n \mid R\rangle$, where R consists of just one element r (see Section 7.8); in other words, $G \cong F/(r)$, where F is a free pro-p group of finite rank, $r \in F$, and (r) denotes the smallest closed normal subgroup of F containing r.

In some analogy with a well-known result of Lyndon [1950] for abstract groups, Serre [1963] posed the following question, slightly corrected by Gildenhuys [1968].

Open Question 7.10.4 *Let G be a finitely generated pro-p group such that $cd(G) > 2$ and $\dim H^2(G, \mathbf{Z}/p\mathbf{Z}) = 1$, i.e., $rr(G) = 1$. Does G admit a presentation with a single defining relator of the form u^p?*

For studies of pro-p groups with one defining relator and connections with Lie algebras and group algebras, see Labute [1967], Romanovskii [1992], Gildenhuys, Ivanov and Kharlampovich [1994]; a 'Freiheitssatz' for pro-p groups appears in Romanovskii [1986]. Somewhat related are the results in Würfel [1986]. For results on finitely presented profinite groups, see Remeslennikov [1979], Myasnikov and Remeslennikov [1987].

7.10.1 Poincaré Groups

Let G be a pro-p group and let n be a natural number. We say that G is a *Poincaré group of dimension n* if the following conditions are satisfied:

(1) $H^i(G)$ is finite for every i;
(2) $\dim H^n(G) = 1$;
(3) $H^i(G) = 0$ for $i > n$; and
(4) For every integer i, $0 \le i \le n$, the cup product

$$H^i(G) \times H^{n-i} \xrightarrow{\cup} H^n(G)$$

is a nondegenerate bilinear form.

According to Theorems 7.7.4 and 7.8.1 and the definition of cup products, the only pro-p Poincaré group of dimension 1 is $\mathbf{Z}_p$.

Poincaré groups of dimension 2 are called *Demushkin groups*. By Theorem 7.8.3, a Demushkin group admits a presentation with a single defining relator. These presentations have been studied in Demushkin [1959, 1963], Serre [1963], Labute [1966a, 1966b], Dummit and Labute [1983]. There is a good presentation of some of these results in Serre [1995]; see also Weigel [2005]. For results on Poincaré groups of dimension 3 see Grunewald, Jaikin-Zapirain, Pinto and Zalesskii [2008].

For the study of general profinite groups satisfying a duality more general than a Poincaré type duality, see the article of Verdier in Serre [1995], Ch. I, Annex 2, and Pletch [1980a, 1980b].

Next we state an unrelated problem due to Ivan Fesenko about finitely generated pro-p groups. The motivation for the problem comes from ramification theory. It is known (due to Abrashkin) that if G_r is a ramification subgroup of the Galois group G of the maximal p-extension of a local field with algebraically closed residue field of characteristic p, then every closed subgroup of infinite index in G/G_r (which itself is an infinite generated pro-p group) is a free pro-p group. Thus, he proposes the following:

Open Question 7.10.5 *Study finitely generated pro-p groups with the following property: every closed subgroup of infinite index is free pro-p.*

In a different direction one can pose (cf. Kochloukova and Zalesskii [2010]) the following

Open Question 7.10.6 *Let F be a free pro-p group of finite rank. Is* $vcd(\mathrm{Aut}(F))$ *finite?*

8 Normal Subgroups of Free Pro-$\mathcal{C}$ Groups

Throughout this chapter $\mathcal{C}$ denotes usually an NE-*formation of finite groups, i.e., $\mathcal{C}$ is a nonempty class of finite groups closed under taking normal subgroups, homomorphic images and extensions. Equivalently, $\mathcal{C}$ is the class of all finite Δ-groups, where Δ is a set of finite simple groups* (*see Section* 2.1). *In particular, $\mathcal{C}$ could be the class of all finite groups, the class of all finite solvable groups, etc. Often we require in addition that $\mathcal{C}$ 'involves two different primes', that is, that there exists a group in $\mathcal{C}$ whose order is divisible by at least two different prime numbers. In this chapter $\Sigma_{\mathcal{C}}$ denotes the collection of all finite simple groups in $\mathcal{C}$, and Σ denotes the class of all finite simple groups.*

The main theme of this chapter is the structure of the closed normal subgroups of a free pro-$\mathcal{C}$ group. In Chapter 7 (Corollary 7.7.5) we saw that all closed subgroups of a free pro-p group are free pro-p. However, for a general class $\mathcal{C}$, the closed subgroups of a free pro-$\mathcal{C}$ group F need not be free pro-$\mathcal{C}$. For example, a p-Sylow subgroup of a free profinite group of rank 2 is not free profinite. Moreover, it is difficult to establish conditions under which closed subgroups of F will be free pro-$\mathcal{C}$, other than being open in F or a certain type of free factors of F (e.g., if Y is a clopen subset of a topological basis X of F, then the closed subgroup of F generated by Y is a free pro-$\mathcal{C}$ group). Nevertheless, we shall see in this chapter that for closed normal subgroups of F, one can describe reasonable conditions to determine whether or not the subgroup is free pro-$\mathcal{C}$. Examples of nonfree normal subgroups of a free pro-$\mathcal{C}$ group can easily be found using, for example, Lemma 3.4.1(e). We shall see, however, that a closed normal subgroup of F is always virtually free pro-$\mathcal{C}$; more precisely we shall see that a proper open subgroup of a closed normal subgroup of F is necessarily free pro-$\mathcal{C}$. Some of the results in the chapter apply not only to normal subgroups of F, but to 'accessible' subgroups, in particular subnormal subgroups of F.

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4_8,

8.1 Normal Subgroup Generated by a Subset of a Basis

Definition 8.1.1 *Let $(Z, *)$ be a pointed topological space and let $(X, *)$ and $(Y, *)$ be pointed subspaces of $(Z, *)$. We say that $(Z, *)$ is the 'coproduct' of $(X, *)$ and $(Y, *)$ if*

(a) $Z = X \cup Y$ *and* $X \cap Y = \{*\}$, *and*
(b) *a subset U is open in Z if and only if $U \cap X$ is open in X and $U \cap Y$ is open in Y.*

Example 8.1.2

(1) Let N be a discrete space and let $Z = N \cupdot \{*\}$ be its one-point compactification. Let $N = N_1 \cupdot N_2$ and set $X = N_1 \cup \{*\}$ and $Y = N_2 \cup \{*\}$. Then $(Z, *)$ is the coproduct of $(X, *)$ and $(Y, *)$.
(2) Let Z' be a profinite space and assume that $Z' = X' \cupdot Y'$ where X' and Y' are clopen subsets of Z'. Let Z be endowed with the unique topology which induces on Z' its original topology and where $*$ is an isolated point. Then $(Z, *)$ is the coproduct of $(X, *) = (X' \cup \{*\}, *)$ and $(Y, *) = (Y' \cup \{*\}, *)$.
(3) Let $(Z, *)$ be a profinite pointed space and let X be a finite subset of Z such that $* \in X$. Set $Y = (Z - X) \cup \{*\}$. Then $(Z, *)$ is the coproduct of $(X, *)$ and $(Y, *)$.

Before stating the main result of this section we need some notation. Assume that a profinite pointed space $(Z, *)$ is the coproduct of two closed pointed subspaces $(X, *)$ and $(Y, *)$. Let $F = F(Z, *)$ be a free pro - $\mathcal{C}$ group on the pointed space $(Z, *)$. Put $G = F(X, *)$, the free pro - $\mathcal{C}$ group on the pointed space $(X, *)$. Consider the product space $G \times Y$, and let $R = (G \times Y)/(G \times \{*\})$ be the quotient space of $G \times Y$ obtained by collapsing the closed subspace $G \times \{*\}$ to a point, which, by abuse of notation, we also denote by $*$. The elements of R are denoted by $\lfloor g, y \rfloor$ $(g \in G, y \in Y)$. We think of R as a pointed space with distinguished point $* = \lfloor g, * \rfloor$. Clearly R is a profinite pointed space. We let G act on the pointed space $(R, *)$ by $g\lfloor g', * \rfloor = \lfloor gg', * \rfloor$; plainly this action is continuous. Then one has

Theorem 8.1.3 *With the notation above, let N be the closed normal subgroup of F generated by Y (i.e., the smallest closed normal subgroup of F containing Y). Then N is a free pro - $\mathcal{C}$ group on the pointed space $(R, *)$. If rank$(F) = \mathfrak{m} > 1$ and $|Y| > 1$, then the rank of N is $\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$.*

Proof. It suffices to prove the first statement, since the second follows from the first (see Proposition 2.6.1).

The action of G on the space $(R, *)$ extends to a continuous action of G on the free pro - $\mathcal{C}$ group $F(R, *)$ (see Exercise 5.6.2(c)). Form the corresponding semidirect product

$$H = F(R, *) \rtimes G.$$

The elements of H can be written as pairs (f,g) $(f \in F(R,*), g \in G)$. Then H is a pro-$\mathcal{C}$ group (see Exercise 5.6.2(b)). Next we define a continuous map of pointed spaces

$$\iota : (Z,*) \longrightarrow H.$$

To do this, it suffices to define its restrictions ι_X and ι_Y to $(X,*)$ and $(Y,*)$, respectively, since $(Z,*)$ is their coproduct. Put

$$\iota_X(x) = (1,x) \quad \text{and} \quad \iota_Y(y) = (\lfloor 1,y \rfloor, 1) \quad (x \in X, y \in Y)$$

(note that in $F(R,*)$, one has $\lfloor g,* \rfloor = * = 1$; while in G, $* = 1$). Since both ι_X and ι_Y are continuous (this is clear since these are really maps into $(R,*) \times G$, and the topology of this space is the product topology), we have that ι is a continuous map of pointed spaces.

We claim that (H,ι) is a free pro-$\mathcal{C}$ group on the pointed space $(Z,*)$. We prove this by checking the universal property of free groups. Let K be a pro-$\mathcal{C}$ group and let $\varphi : (Z,*) \longrightarrow K$ be a continuous map of pointed spaces such that $\varphi(Z,*)$ generates K. Denote by φ_X the restriction of φ to X. Let

$$\bar{\varphi}_X : G = F(X,*) \longrightarrow K$$

be the induced continuous homomorphism; such homomorphism exists, even if $\varphi_X(X)$ does not generate K: it is the restriction of the continuous homomorphism $\bar{\varphi} : F(Z,*) \longrightarrow K$ induced by φ. Define

$$\rho : (R,*) \longrightarrow K$$

by

$$\rho(\lfloor g,y \rfloor) = \bar{\varphi}_X(g)\varphi(y)\bar{\varphi}_X(g^{-1}) \quad (g \in G, y \in Y).$$

We shall prove that $\rho(R,*)$ generates a subgroup L of K which is pro-$\mathcal{C}$. To do that, set $K_X = \langle \bar{\varphi}(X) \rangle$ and $K_Y = \langle \bar{\varphi}(Y) \rangle$. Since K_X and K_Y are homomorphic images of $F(X,*)$ and $F(Y,*)$, respectively, they are pro-$\mathcal{C}$ groups. Note that $\rho(R,*)$ is generated by

$$\{a^b = b^{-1}ab \mid a \in K_X, b \in K_Y\};$$

hence $\rho(R,*)$ is a normal subgroup of K, because K is generated by K_X and K_Y. If follows that L is a pro-$\mathcal{C}$ group (see Proposition 2.2.1).

One sees without difficulty that ρ is a continuous map of pointed spaces. Hence, there exists an induced continuous homomorphism

$$\bar{\rho} : F(R,*) \longrightarrow L \hookrightarrow K.$$

The homomorphisms $\bar{\varphi}_X$ and $\bar{\rho}$ are compatible with the action of G on $F(R,*)$, i.e.,

$$\bar{\rho}(g \cdot f) = \bar{\varphi}_X(g)\varphi(y)\bar{\varphi}_X(g^{-1}) \quad (f \in F(R,*), g \in G).$$

Indeed, this is certainly the case if $f \in R$, by definition; hence it is always true since the action of G on $F(R,*)$ is induced by its action on the basis $(R,*)$ of $F(R,*)$ (see Exercise 5.6.2).

Therefore, the map $\bar{\varphi} : H = F(R,*) \rtimes G \longrightarrow K$ given by

$$\bar{\varphi}(f,g) = \bar{\rho}(f)\bar{\varphi}_X(g),$$

is a continuous homomorphism. Finally, observe that $\bar{\varphi}\iota = \varphi$. This proves the claim.

Thus we can identify H with $F(Z,*)$. Under this identification, Y corresponds to $\{\lfloor 1,y \rfloor \mid y \in Y\}$ in H. By definition of the action of G, the closed normal subgroup N of H generated by $\{\lfloor 1,y \rfloor \mid y \in Y\}$ contains

$$R = \{\lfloor g,y \rfloor \mid y \in Y, g \in G\}.$$

Hence, $N = F(R,*)$, as desired. □

8.2 The S-rank

This section is of a technical nature. Here we introduce the concept of S-rank of a group, where S is a finite simple group. In the next sections we shall use the idea of S-rank to characterize which profinite groups appear as normal, characteristic or subnormal subgroups of a free pro - $\mathcal{C}$ group; or, more generally, as 'accessible' (see Section 8.3) or 'homogeneous' (see Section 8.4) subgroups of a free pro - $\mathcal{C}$ group.

Lemma 8.2.1 *Let G be a profinite group and let K be an open normal subgroup of G such that G/K is a nonabelian finite simple group. Let $\mathcal{M}$ be the set of all closed normal subgroups M of G for which $MK = G$. Then $\mathcal{M}$ is closed under arbitrary intersections, i.e., the intersection of any collection of groups in $\mathcal{M}$ is in $\mathcal{M}$.*

Proof. We show first that if $M_1, M_2 \in \mathcal{M}$, then $M_1 \cap M_2 \in \mathcal{M}$. Suppose not, that is, suppose that $(M_1 \cap M_2)K \neq G$. Since G/K is simple, we have $M_1 \cap M_2 \leq K$. Consider arbitrary elements $a, b \in M_1$. Since $M_2K = G$, there exist $m \in M_2$ and $k \in K$ with $a = mk$. Then, using elementary commutator calculus,

$$[a,b] = [mk,b] = (mk)^{-1}b^{-1}mkb = [k,b^m][m,b].$$

Since $[m,b] \in K$, it follows that $[a,b] \in K$. Thus,

$$G/K = M_1K/K \cong M_1/M_1 \cap K$$

is abelian, a contradiction. This implies that $M_1 \cap M_2 \in \mathcal{M}$, as desired. Therefore $\mathcal{M}$ is closed under finite intersections.

Now let $\mathcal{L}$ be an arbitrary subset of $\mathcal{M}$, and put $L = \bigcap_{M \in \mathcal{L}} M$. We need to prove that $LK = G$. Fix $g \in G$ and define $B_M = M \cap gK$, for $M \in \mathcal{L}$. It follows from the first part of the proof that the family $\{B_M \mid M \in \mathcal{L}\}$ of closed subsets of G has the finite intersection property. Thus the intersection of all the subsets in this family is nonempty by the compactness of G. Therefore $L \cap gK \neq \emptyset$. So $g \in LK$. Hence $LK = G$, as needed. □

Lemma 8.2.2 *Let G be a profinite group and let $\mathcal{M} \supseteq \mathcal{M}'$ be sets of maximal open normal subgroups of G. Put $M = \bigcap_{R \in \mathcal{M}} R$. Assume that the natural homomorphism*

$$\varphi(\mathcal{M}') : G \longrightarrow \prod_{R \in \mathcal{M}'} G/R$$

is an epimorphism. Then there exists a subset $\mathcal{N}$ of $\mathcal{M}$ containing $\mathcal{M}'$ such that the natural homomorphism

$$\varphi(\mathcal{N}) : G \longrightarrow \prod_{R \in \mathcal{N}} G/R$$

is an epimorphism and $M = \mathrm{Ker}(\varphi(\mathcal{N}))$, i.e.,

$$G/M \cong \prod_{R \in \mathcal{N}} G/R.$$

Proof. Let Ω be the family of all subsets $\mathcal{L}$ of $\mathcal{M}$ such that $\mathcal{M}' \subseteq \mathcal{L}$ and

$$\varphi(\mathcal{L}) : G \longrightarrow \prod_{R \in \mathcal{L}} G/R$$

is an epimorphism. The family Ω is nonempty because $\mathcal{M}'$ belongs to Ω. Since $\prod_{R \in \mathcal{L}} G/R$ is an inverse limit of direct products over finite sets (see Exercise 1.1.14), one deduces from Corollary 1.1.6 that $\mathcal{L} \in \Omega$ if and only if $\varphi(\mathcal{F})$ is an epimorphism for each of its finite subsets $\mathcal{F}$. Therefore Ω, ordered by inclusion, is an inductive set. Hence there exists a maximal $\mathcal{N}$ in Ω by Zorn's Lemma. To finish the proof it suffices to show that $M = \mathrm{Ker}(\varphi(\mathcal{N}))$. Put $N = \bigcap_{R \in \mathcal{N}} R$. We must show that $N = M$. It is obvious that $M \leq N$. If $M < N$, then there would exist some $K \in \mathcal{M}$ with $K \cap N < N$. So, since G/K is simple, $KN = G$, and hence $G/K \cap N \cong G/K \times G/N$. This would imply that $\mathcal{N} \cup \{K\} \in \Omega$, contrary to the maximality of $\mathcal{N}$. Thus $N = M$, as desired. □

Lemma 8.2.3 *Let G be a profinite group and let $\mathcal{M}$ be a set of maximal open normal subgroups of G such that G/R is a nonabelian finite simple group for every $R \in \mathcal{M}$. Put $M = \bigcap_{R \in \mathcal{M}} R$. Then the natural homomorphism*

$$\varphi : G/M \longrightarrow \prod_{R \in \mathcal{M}} G/R$$

is an isomorphism.

Proof. Consider first the case when $\mathcal{M}$ is finite, say $\mathcal{M} = \{M_1, \dots, M_n\}$. If $n = 1$, the result is obvious. If $n > 1$, we use induction. Let $R' = M_2 \cap \cdots \cap M_n$ and assume that $G/R' = G/M_2 \times \cdots \times G/M_n$. We need to show that the natural homomorphism $\tilde{\varphi} : G \longrightarrow G/M_1 \times G/R'$ is an epimorphism. By Lemma 8.2.1, $M_1 R' = G$. Let $g, g' \in G$. Then $gM_1 = r'M_1$, for some $r' \in R'$, and $g'R' = m_1 R'$, for some $m_1 \in M_1$. So $\tilde{\varphi}(r'm_1) = (gM_1, g'R')$, i.e., $\tilde{\varphi}$ is an epimorphism. This proves the result when $\mathcal{M}$ is finite.

For the general case, observe that φ is in a natural way the inverse limit of the isomorphisms

$$\varphi_{\mathcal{N}} : G/N \longrightarrow \prod_{R \in \mathcal{N}} G/R,$$

where $\mathcal{N}$ ranges over the finite subsets of $\mathcal{M}$, and where $N = \bigcap_{R \in \mathcal{N}} R$. □

Lemma 8.2.4 *Let $\{S_i \mid i \in I\}$ be a family of finite simple groups and let*

$$G = \prod_{i \in I} S_i.$$

Set $I_a = \{i \in I \mid S_i \text{ is abelian}\}$ and $I_n = \{i \in I \mid S_i \text{ is nonabelian}\}$. Define

$$G_a = \prod_{i \in I_a} S_i \quad \text{and} \quad G_n = \prod_{i \in I_n} S_i.$$

(a) *Let $K \triangleleft G$. Assume that S_j is nonabelian (some $j \in I$). Then $S_j \leq K$ if and only if $\pi_j(K) \neq 1$, where $\pi_j : G \longrightarrow S_j$ denotes the canonical projection.*
(b) *If $K \triangleleft G$ and S_i is not abelian for each $i \in I$, then*

$$K = \prod_{i \in I'} S_i,$$

where $I' = \{i \in I \mid \pi_i(K) \neq 1\}$.
(c) *If $K \triangleleft G$, then $K = (K \cap G_a) \times (K \cap G_n)$.*
(d) *Let K be a closed normal subgroup of G considered as a profinite group. Then both K and G/K are a direct product of finite simple groups; moreover, there is a continuous isomorphism $G \cong K \times G/K$.*
(e) *Assume that $\{G_i \mid i \in I\}$ and $\{H_j \mid j \in J\}$ are families of finite simple groups such that*

$$\prod_{i \in I} G_i \cong \prod_{j \in J} H_j.$$

Then $|I| = |J|$.

Proof. (a) In one direction the result is obvious. Assume $\pi_j(K) \neq 1$. Then there exists some $k = (k_i) \in K$ with $k_j \neq 1$. To see that $G_j \leq K$, it suffices to prove that $G_j \cap K \neq 1$. Since the center of G_j is trivial, there exists some

$t \in G_j$ such that $t^{-1}k_jt \neq k_j$. Define $g = (g_i)$ to be the element of G such that $g_i = 1$, if $i \neq j$, and $g_j = t$. Then $1 \neq k^{-1}g^{-1}kg \in G_{i'} \cap K$, as needed.

Parts (b) and (c) follow easily from (a).

(d) By part (b),

$$G_n = (G_n \cap K) \times \left(\prod_{i \in I_a - I'} S_i \right).$$

Next, denote G_a by L and $G_a \cap K$ by R. For each prime number p, let L_p and R_p denote the unique p-Sylow subgroups of L and R, respectively. Then $L = \prod_p L_p$, $R = \prod_p R_p$ and $R_p \leq_c L_p$. Observe that L_p and R_p are direct products of copies of a cyclic group of order p. By Proposition 2.8.16, $L_p = R_p \times {R_p}'$, where ${R_p}'$ is a closed subgroup of L_p. Hence ${L_p}'$ is a direct product of copies of a cyclic group of order p. Put $R' = \prod_p {R_p}'$. Then

$$G_a = L = R \times R' = (G_a \cap K) \times R'.$$

Using this and part (c), we deduce that K has a closed complement $K' = R' \times (\prod_{i \in I_a - I'} S_i)$ in G and both K and K' are direct products of finite simple groups. Since $K' \cong G/K$, all statements in part (d) follow.

(e) It is plain that either I and J are both finite or both infinite. If both are finite, the result is a consequence of the Krull-Remak-Schmidt theorem (cf. Huppert [1967], Satz I.12.3). Suppose that I and J are both infinite.Then $2^{|I|} = |G| = |H| = 2^{|J|}$. Hence $|I| = |J|$. □

Let S be a fixed finite simple group and let G be a profinite group. Denote by $M_S(G)$ the intersection of all closed normal subgroups N of G whose quotient group G/N is isomorphic to S. By Lemma 8.2.2,

$$G/M_S(G) \cong \prod_I S,$$

the direct product of $|I|$ copies of S, where I is some indexing set. The S-*rank* $r_S(G)$ of G is defined to be the cardinality of the indexing set I. This is well-defined by Lemma 8.2.4(e). Observe that if S does not appear as a quotient of G, then $r_S(G) = 0$. If $S \cong \mathbf{Z}/p\mathbf{Z}$, where p is a prime number, we write $r_p(G)$ instead of $r_S(G)$, and we refer to it as the p-*rank* of G.

Lemma 8.2.5 *Let S be a finite simple group and let G be a profinite group.*

(a) $r_S(K) \leq \max\{w_0(G), \aleph_0\}$, *for each closed subgroup K of G.*
(b) *If H is a continuous homomorphic image of G, then $r_S(H) \leq r_S(G)$.*
(c) $r_S(G) = r_S(G/M_S(G))$.
(d) *If $K \triangleleft_c G$, then $r_S(G) \leq r_S(K) + r_S(G/K)$.*

Proof. Parts (a), (b) and (c) are clear. We show (d). It follows from Lemma 8.2.4(b) that $G/M_S(G) \cong G/KM_S(G) \times KM_S(G)/M_S(G)$. On the other hand, there exist natural epimorphisms

$$G/K \longrightarrow G/KM_S(G)$$

and

$$K/M_S(K) \longrightarrow K/K \cap M_S(G) \cong KM_S(G)/M_S(G).$$

Hence the result is a consequence of part (b). □

Proposition 8.2.6 *Assume that $\mathcal{C}$ is a formation of finite groups. Let $F = F_{\mathcal{C}}(X)$ be a free pro - $\mathcal{C}$ group of infinite rank $\mathfrak{m}$. Then $r_S(F) = \mathfrak{m}$ for every finite simple group $S \in \mathcal{C}$.*

Proof. By Proposition 2.6.2, $\mathfrak{m} = w_0(F)$. Then $r_S(F) \leq \mathfrak{m}$, according to Lemma 8.2.5(a). Let I be a set of cardinality $\mathfrak{m}$. Since $d(\prod_I S) = \mathfrak{m}$, there exists an epimorphism $F \longrightarrow \prod_I S$. Hence, Lemma 8.2.5(b) implies that $r_S(F) \geq \mathfrak{m}$. □

Lemma 8.2.7 *Let n and m be natural numbers. Denote by $F_{\mathcal{C}}(n)$ the free pro - $\mathcal{C}$ group of rank n.*

(a) *If p is a prime number and $\mathbf{Z}/p\mathbf{Z} \in \mathcal{C}$, then $r_p(F_{\mathcal{C}}(n)) = n$.*
(b) *If $S \in \mathcal{C}$ is a simple nonabelian group and $n \geq d(S)$,* * *then*

$$r_S(F_{\mathcal{C}}(n+1)) \geq 2r_S(F_{\mathcal{C}}(n)).$$

(c) *If $S \in \mathcal{C}$ is a simple nonabelian group and $m > n \geq \mathrm{d}(S)$, then*

$$r_S(F_{\mathcal{C}}(m)) - r_S(F_{\mathcal{C}}(n)) \geq m - n.$$

Proof. (a) Consider the group $A = \langle a_1 \rangle \times \cdots \times \langle a_n \rangle$, where $\langle a_i \rangle \cong \mathbf{Z}/p\mathbf{Z}$ $(i = 1, \ldots, n)$. Say that $X = \{x_1, \ldots, x_n\}$ is a basis for the group $F = F_{\mathcal{C}}(n)$, and let

$$\pi : F \longrightarrow A$$

be the epimorphism defined by $\pi(x_i) = a_i$ $(i = 1, \ldots, n)$. Every epimorphism

$$\varphi : F \longrightarrow \mathbf{Z}/p\mathbf{Z}$$

factors through π; so, if $L \triangleleft_o F$ and $F/L \cong \mathbf{Z}/p\mathbf{Z}$, there exists some subgroup L' of A of index p such that $\pi^{-1}(L') = L$. It follows that

$$\begin{aligned} M_p(F) &= \bigcap \{L \mid L \triangleleft_o F, F/L \cong \mathbf{Z}/p\mathbf{Z}\} \\ &= \pi^{-1}\left(\bigcap \{L' \mid L' \leq A, A/L' \cong \mathbf{Z}/p\mathbf{Z}\}\right) = \mathrm{Ker}(\pi). \end{aligned}$$

Hence $F/M_p(F) = A$, and therefore $r_p(F_{\mathcal{C}}(n)) = n$.

(b) Put

$$E(n) = F_{\mathcal{C}}(n)/M_S(F_{\mathcal{C}}(n)) \cong \prod_{i \in I} S,$$

* It follows from the classification of finite simple groups that $d(S) = 2$ for all nonabelian finite simple groups S.

where $|I| = \mathrm{r}_S(F_{\mathcal{C}}(n))$. Let v be an element of $E(n)$ whose projection onto each of the direct factors of $\prod_{i\in I} S$ is nontrivial; let w be the preimage of v in $F_{\mathcal{C}}(n)$; and let $\{x_1, \dots, x_n\}$ and $\{y_1, \dots, y_{n+1}\}$ be bases of $F_{\mathcal{C}}(n)$ and $F_{\mathcal{C}}(n+1)$, respectively. Define epimorphisms

$$\varphi, \psi : F_{\mathcal{C}}(n+1) \longrightarrow F_{\mathcal{C}}(n)$$

by $\varphi(y_i) = \psi(y_i) = x_i$ for $i = 1, \dots, n$, $\varphi(y_{n+1}) = w$ and $\psi(y_{n+1}) = 1$.

$$\begin{array}{ccc} F_{\mathcal{C}}(n+1) & \longrightarrow & E(n+1) \\ {\scriptstyle\varphi}\big\downarrow{\scriptstyle\psi} & & {\scriptstyle\alpha}\big\downarrow{\scriptstyle\beta} \\ F_{\mathcal{C}}(n) & \longrightarrow & E(n) \end{array}$$

Denote by K the normal subgroup of $E(n+1)$ generated by the image of y_{n+1} under the natural projection

$$F_{\mathcal{C}}(n+1) \longrightarrow E(n+1),$$

and let

$$\alpha, \beta : E(n+1) \longrightarrow E(n)$$

be the epimorphisms induced by φ and ψ respectively. Since S is simple nonabelian, we infer from the choice of v, that v generates $E(n)$ as a normal subgroup (see Lemma 8.2.4). It follows that $\alpha(K) = E(n)$. On the other hand, $\beta(K) = 1$; therefore, β induces an epimorphism from $E(n+1)/K$ onto $E(n)$. Thus, since K is a direct factor of $E(n+1)$ (see Lemma 8.2.4(c)), we have

$$\begin{aligned} r_S(F_{\mathcal{C}}(n+1)) &= r_S(E(n+1)) \\ &= r_S(K) + r_S(E(n+1)/K) \geq 2r_S(E(n)) = 2r_S(F_{\mathcal{C}}(n)). \end{aligned}$$

(c) Since $n \geq \mathrm{d}(S)$, we deduce from (b) that

$$r_S(F_{\mathcal{C}}(n+1)) - r_S(F_{\mathcal{C}}(n)) \geq 1.$$

Hence

$$r_S(F_{\mathcal{C}}(m)) - r_S(F_{\mathcal{C}}(n)) \geq m - n,$$

by induction on $m - n$. □

Exercise 8.2.8 Let G be a profinite group.

(1) Let p be a prime number. Then $r_p(G) = 0$ if and only if $H^1(G, \mathbf{Z}/p\mathbf{Z}) = 0$, where $\mathbf{Z}/p\mathbf{Z}$ is considered as a trivial G-module.
(2) $r_p(G) = 0$ for all prime p if and only if $H^1(G, \mathbf{Q}/\mathbf{Z}) = 0$, where $\mathbf{Q}/\mathbf{Z}$ is considered as a trivial G-module.
(3) Let $F = F(n)$ be the free profinite group of finite rank n, $\tilde{F} = F_{Sol}(n)$ the free prosolvable group of rank n and $\varphi : F \longrightarrow \tilde{F}$ the canonical epimorphism. Then $r_p(\mathrm{Ker}(\varphi)) = 0$ for every prime p.

8.3 Accessible Subgroups

A closed subgroup H of a profinite group G is said to be *accessible* if there exists a chain of closed subgroups of G

$$H = G_\mu \leq \cdots \leq G_\lambda \leq \cdots \leq G_2 \leq G_1 = G, \tag{1}$$

indexed by the ordinals smaller than a certain ordinal μ, such that

(i) $G_{\lambda+1} \triangleleft G_\lambda$ for all ordinals $\lambda \leq \mu$, and
(ii) if ν is a limit ordinal such that $\nu \leq \mu$, then $G_\nu = \bigcap_{\lambda \leq \nu} G_\lambda$.

A chain with properties (i) and (ii) will be called an *accessible chain* of H in G.

Clearly, a closed subnormal subgroup is accessible since it has a finite accessible chain. We collect some basic properties of accessible subgroups in the following

Proposition 8.3.1 *Let H be an accessible subgroup of a profinite group G. Then*

(a) *If N is an accessible subgroup of H, then N is an accessible subgroup of G.*
(b) *For any subgroup L of G, the intersection $H \cap L$ is an accessible subgroup of L.*
(c) *For any continuous epimorphism $\varphi : G \longrightarrow K$ of profinite groups, the image $\varphi(H)$ of H is an accessible subgroup of K.*

Proof. Parts (a) and (b) follow directly from the definition of an accessible subgroup. For (c), let (1) be an accessible chain of H in G. Then

$$\varphi(H) = \varphi(G_\mu) \leq \cdots \leq \varphi(G_\lambda) \leq \cdots \leq \varphi(G_2) \leq \varphi(G_1) = K$$

is also an accessible chain. Indeed, it is plain that $\varphi(G_{\lambda+1}) \triangleleft \varphi(G_\lambda)$. Let ν be a limit ordinal with $\nu \leq \mu$. Then, by Proposition 2.1.4(b),

$$\bigcap_{\lambda \leq \nu} \varphi(G_\lambda) = \varphi(G_\nu).$$

□

The next theorem gives useful characterizations of accessible subgroups of a profinite group.

Theorem 8.3.2 *Let H be a closed subgroup of a profinite group G. Define a chain of subgroups indexed by the natural numbers*

$$G = N_1 \triangleright N_2 \triangleright \cdots$$

as follows: $N_1 = G$, and if N_m has been already defined, let N_{m+1} be the normal closure of H in N_m (that is, the smallest closed normal subgroup of N_m containing H). Then the following statements are equivalent.

(a) *H is accessible in G*;
(b) *The image of H in every finite quotient group of G is subnormal*;
(c) $H = \bigcap_{m=1}^{\infty} N_m$.

Proof. The implication (a) ⇒ (b) follows from Proposition 8.3.1(c) and the fact that every accessible subgroup of a finite group is subnormal.

(b) ⇒ (c): Write G as an inverse limit $G = \varprojlim G_i$ of a surjective inverse system $\{G_i, \varphi_{ij}, I\}$ of finite groups. Let $\varphi_i : G \longrightarrow G_i$ be the projection, and set $H_i = \varphi_i(H)$ $(i \in I)$. Choose a subnormal chain of H_i in G_i

$$G_i = G_{i1} \rhd G_{i2} \rhd \cdots \rhd G_{in_i} = H_i.$$

Obviously $\varphi_i(N_1) = G_{i1}$. Since φ_i is an epimorphism, one has that $\varphi_i(N_{m+1})$ is the normal closure of H_i in $\varphi_i(N_m)$, for every natural number m. Hence one can argue by induction on m to deduce that $\varphi_i(N_m) \leq G_{im}$ for all $m = 1, 2, \ldots, n_i$. Therefore, $\varphi_i(N_k) = H_i$, for $k \geq n_i$. Put

$$N = \bigcap_{m=1}^{\infty} N_m.$$

By Proposition 2.1.4(b), one has $\varphi_i(N) = H_i = \varphi_i(H)$, for all $i \in I$. Then, by Corollary 1.1.8, $H = N = \bigcap_{i=1}^{\infty} N_i$, as required.

The implication (c) ⇒ (a) is obvious. □

Corollary 8.3.3 *Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups. Then every accessible subgroup of a pro-$\mathcal{C}$ group is a pro-$\mathcal{C}$ group.*

Corollary 8.3.4 *Let p be a prime number and let G be a pro-p group* (*or, more generally*, *a pronilpotent group*). *Then every closed subgroup of G is accessible.*

Proof. This follows from part (b) of the above theorem since in a finite p-group (more generally, in a finite nilpotent group), every subgroup is subnormal (cf. Hall [1959], Corollary 10.3.1). □

This corollary shows that the concept of accessible subgroup plays no role in the study of pro-p groups. It explains why whenever accessible groups are involved in this and subsequent sections, we shall assume that those groups are, in general, not pro-p.

The characterizations given in Theorem 8.3.2 are very useful in proving properties related to accessible groups. We begin with the following

Proposition 8.3.5

(a) *Let $\{H_i \mid i \in I\}$ be a family of accessible subgroups of a profinite group G. Then their intersection $H = \bigcap_{i\in I} H_i$ is an accessible subgroup of G.*

(b) *If H_1 and H_2 are accessible subgroups of a profinite group G, then the subgroup $H = \overline{\langle H_1, H_2\rangle}$ generated by H_1 and H_2 is also accessible.*

Proof. (a) Let $\mathcal{F}$ be the collection of all finite subsets of I. For $F \in \mathcal{F}$, put $H_F = \bigcap_{i\in F} H_i$. Let us show that H_F is accessible in G, for every $F \in \mathcal{F}$. By an obvious induction, we may assume that F consists of two elements i and j. Remark that $H_i \cap H_j$ is accessible in H_j by Proposition 8.3.1(b). Since H_j is accessible in G, then $H_i \cap H_j$ is accessible in G by Proposition 8.3.1(a).

Note that

$$H = \bigcap_{F\in\mathcal{F}} H_F.$$

Let $\varphi : G \longrightarrow K$ be a continuous epimorphism onto a finite group K. Since the collection of subgroups $\{H_F \mid F \in \mathcal{F}\}$ is filtered from below, one has

$$\varphi(H) = \bigcap_{F\in\mathcal{F}} \varphi(H_F)$$

(see Proposition 2.1.4(b)). Since K is finite, one deduces that $\varphi(H)$ is subnormal in K. Then H is accessible in G by Theorem 8.3.2.

(b) Let $\varphi : G \longrightarrow K$ be a continuous epimorphism onto a finite group K. Clearly $\varphi(H_1)$ and $\varphi(H_2)$ are subnormal in K. Furthermore, $\varphi(H)$ is generated by $\varphi(H_1)$ and $\varphi(H_2)$. Now, a subgroup generated by subnormal subgroups is subnormal (cf. Suzuki [1982], Ch. 2, 3.23). Hence, by Theorem 8.3.2, H is accessible in G. □

Let G be a profinite group. We denote by $M(G)$ the intersection of all maximal closed normal subgroups of G. Next we show that $M(G)$ has a Frattini type property with respect to accessible subgroups.

Proposition 8.3.6 *Let H be an accessible group of a profinite group G. If $HM(G) = G$, then $H = G$.*

Proof. Assume first that H is normal in G. If $H \neq G$, then H is contained in some closed maximal normal subgroup M of G. But $M(G) \subseteq M$; therefore $HM(G) \leq M < G$, a contradiction.

Next consider the general case. Let N be the normal closure of H in G. We claim that $N = G$ if and only if $H = G$. Indeed, if $N = G$, then, using the notation of Theorem 8.3.2, we have that $N_i = G$ for all $i = 1, 2, \dots$, by induction. Hence $H = \bigcap_{i=1}^{\infty} N_i = G$. The converse is obvious.

Since $H \leq N$, then $HM(G) = G$ implies $NM(G) = G$. By the first part of the proof, $N = G$. Thus from above, $H = G$. □

We end this section with two technical results that will be of use later.

Lemma 8.3.7 *Let $\varphi : G \longrightarrow H$ be a continuous epimorphism of profinite groups. Then $\varphi(M(G)) = M(H)$.*

Proof. Since φ^{-1} sends maximal closed normal subgroups of H to maximal closed normal subgroups of G and since φ^{-1} preserves intersections, we have that $\varphi^{-1}(M(H)) \geq M(G)$. So, $\varphi(M(G)) \leq M(H)$. For the reverse containment, observe that $H/\varphi(M(G))$ is a direct product of finite simple groups, since it is a homomorphic image of $G/M(G)$ (see Lemma 8.2.4(d)). Therefore, $\varphi(M(G))$ is an intersection of maximal closed normal subgroups of H. Thus, $\varphi(M(G)) \geq M(H)$. □

The following lemma shows how certain information on subgroups placed deep in a profinite group can be brought closer to the surface of the group. This lemma plays a crucial role in many of the results in this chapter.

Lemma 8.3.8 *Let $\mathcal{C}$ be a formation of finite groups which is also closed under taking normal subgroups. Let H and K be subgroups of a pro-$\mathcal{C}$ group G with $K \triangleleft_c H$, and assume that H is an accessible subgroup of G. Then G has a closed pro-$\mathcal{C}$ subgroup L containing H such that*

(1) *L is an accessible subgroup of G;*
(2) *there exists a continuous epimorphism $\rho : L \longrightarrow H/K$ extending the canonical epimorphism $H \longrightarrow H/K$; and*
(3) *$w_0(G/L) \leq w_0(H/K)$ (note that G/L is not necessarily a group).*

Moreover,

(a) *if $[G : H] = \infty$ and $[H : K] < \infty$, then L is open. Furthermore, any open subnormal subgroup L' of L containing H also satisfies conditions* (1)–(3); *in addition, such L' can be chosen so that it has arbitrarily large finite index in G;*
(b) *if $H \triangleleft_c G$, then $L \triangleleft_c G$, $K \triangleleft_c L$ and $L/K \cong H/K \times \mathrm{Ker}(\rho)/K$; and*
(c) *if $H \triangleleft_c G$ and $K \triangleleft_c G$, then $\mathrm{Ker}(\rho) \triangleleft_c G$.*

Proof. Since accessible subgroups of pro-$\mathcal{C}$ groups are pro-$\mathcal{C}$ (see Corollary 8.3.3), we have that both H and K are pro-$\mathcal{C}$ groups. Let $\{U_i \mid i \in I\}$ be a family of open normal subgroup of H such that $\bigcap_{i\in I} U_i = K$ and $|I| = w_0(H/K)$. For each $i \in I$, choose $V_i \triangleleft_o G$ with $H \cap V_i \leq U_i$. Put $V = \bigcap_{i\in I} V_i$. Define $L = HV$. In light of Proposition 8.3.5, L is an accessible subgroup of G; so L is pro-$\mathcal{C}$ (see Corollary 8.3.3). By Proposition 2.1.5, the set of all finite intersections of the open subgroups $\{V_i/V \mid i \in I\}$ form a fundamental system of neighborhoods of G/V; hence $w_0(G/V) \leq |I|$. Therefore, $w_0(G/L) \leq |I| = w_0(H/K)$, because G/L is a quotient space of G/V. Since $KV \triangleleft HV = L$ and $V \cap H \leq K$, we have

$$L/KV = HKV/KV \cong H/H \cap (KV) \cong H/K.$$

Define $\rho : L \longrightarrow H/K$ to be the composition of natural maps

$$L \longrightarrow L/KV \xrightarrow{\cong} H/K.$$

Plainly ρ is an epimorphism and its restriction to H is the natural epimorphism $H \longrightarrow H/K$. Hence we have shown that L satisfies conditions (1), (2) and (3).

(a) Assume now that $[G : H] = \infty$ and $[H : K] < \infty$. Let L be the group constructed above. Then $w_0(G/L) \leq w_0(H/K) = 1$; so L is open in G. Let r be a natural number; since H is an accessible subgroup of L, there exists an open subnormal subgroup L' of L with $H \leq L'$ and such that $[G : L'] \geq r$. Fix any such L'. Obviously L' is an accessible subgroup of G; hence L' is pro-$\mathcal{C}$. Note that $L'V = L = HV$. Thus

$$L' \longrightarrow L'V/KV \xrightarrow{\cong} H/K$$

is an epimorphism extending $H \longrightarrow H/K$.

(b) Assume that $H \triangleleft_c G$. Then clearly $L = HV \triangleleft_c G$. On the other hand,

$$\overline{[V,K]} \leq V \cap H = \left(\bigcap_{i \in I} V_i\right) \cap H = \bigcap_{i \in I}(V_i \cap H) = \bigcap_{i \in I} U_i = K,$$

where $\overline{[V,K]}$ is the closed subgroup generated by the commutators $[v,k]$ ($v \in V, k \in K$). Therefore, V normalizes K. Thus $K \triangleleft_c HV = L$. Finally, observe that $\mathrm{Ker}(\rho) = KV$; so $H \cap \mathrm{Ker}(\rho) = K$. Hence $L/K \cong H/K \times \mathrm{Ker}(\rho)/K$.

(c) If $H \triangleleft_c G$ and $K \triangleleft_c G$, note that then $\mathrm{Ker}(\rho) = KV \triangleleft_c G$. □

Exercise 8.3.9 Let $\mathcal{C}$ be an extension closed variety of finite groups. Let H and K be closed subgroups of a pro-$\mathcal{C}$ group G with $K \triangleleft H$. Then G has a closed subgroup L containing H such that

(1) there is a continuous epimorphism $\rho : L \longrightarrow H/K$ extending the canonical epimorphism $H \longrightarrow H/K$; and
(2) $w_0(G/L) \leq w_0(H/K)$ (note that G/L is not necessarily a group).

Exercise 8.3.10 Let K be a minimal finite normal subgroup of a profinite group G. Then $K \leq M(G)$ if and only if G does not split as a direct product $G \cong K \times G/K$. [Hint: use Lemma 8.2.4(d).]

8.4 Accessible Subgroups H with $w_0(F/H) < \mathrm{rank}(F)$

In Theorem 3.6.2 we saw that open subgroups of free pro-$\mathcal{C}$ groups are free pro-$\mathcal{C}$ if $\mathcal{C}$ is an extension closed variety of finite groups, that is, freeness is preserved for groups that are "close to the surface" of F. In this section we pursue this idea of being close to the surface relative to the rank of the free group. The main result is that if H is an accessible subgroup of infinite index in a free pro-$\mathcal{C}$ group F and $w_0(F/H)$ is sufficiently small in relation to the rank of F, then H is also free pro-$\mathcal{C}$.

Lemma 8.4.1 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let F be a free pro-$\mathcal{C}$ group of finite rank $n \geq 2$ and assume that K is a closed normal subgroup of F of infinite index such that $d(F/K) < n$. Let r be a natural number. Then there exists an open normal subgroup L_r of F containing K such that for every open subgroup U of F with $K \leq U \triangleleft L_r$, one has*

$$\mathrm{rank}(U) - d(U/K) \geq r.$$

Proof. We proceed by induction on r. For $r = 1$, choose $L_1 = F$; the result then follows from Corollary 3.6.3 and Theorem 3.6.2. For a given $r \geq 1$, assume the existence of L_r satisfying the conditions of the lemma. Define L_{r+1} to be a proper open subgroup of L_r containing K such that $L_r \triangleleft F$. Let U be an open subgroup of F with $K \leq U \triangleleft L_{r+1}$. Then, using Theorem 3.6.2, Corollary 3.6.3 and the induction hypothesis, we have

$$\begin{aligned}\mathrm{rank}(U) &= 1 + [L_r : U](\mathrm{rank}(L_r) - 1) \geq 1 + [L_r : U](d(L_r/K) + r - 1)\\ &= 1 + [L_r : U](d(L_r/K) - 1) + [L_r : U]r \geq d(U/K) + (r+1),\end{aligned}$$

since $[L_r : U] > 1$. □

In Theorem 3.6.2 we studied subgroups of finite index of a free pro-$\mathcal{C}$ group. The next theorem considers certain accessible subgroups of infinite index which are also free (see Theorem 8.9.4 for further results in this direction).

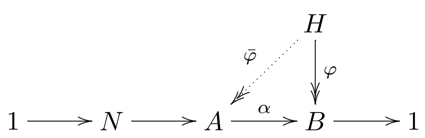
Theorem 8.4.2 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let F be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Set $\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$.*

(a) *Suppose that H is an accessible subgroup of F of infinite index with $w_0(F/H) < \mathfrak{m}$ (note that F/H is not necessarily a group). Then H is a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}^*$.*
(b) *Suppose that H is a closed normal subgroup of F of infinite index with $d(F/H) < \mathfrak{m}$. Then H is a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}^*$.*

Proof. Let $\mathcal{E} = \mathcal{E}_{\mathcal{C}}$ be the class of all epimorphisms of pro-$\mathcal{C}$ groups.

(a) In this case we may assume that $\mathfrak{m} > \aleph_0$, for otherwise H would have finite index. By Corollary 8.3.3 H is a pro-$\mathcal{C}$ group. Observe that $w_0(H) = \mathfrak{m} = \mathfrak{m}^*$, since $w_0(F/H) < \mathfrak{m} = \mathfrak{m}^*$.

Consider the following $\mathcal{E}$-embedding problem for H

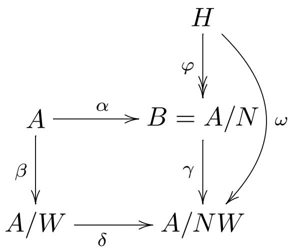


(2)

with $w_0(B) < w_0(H)$, $w_0(A) \leq w_0(H)$ and where the row is exact. We shall show the existence of an epimorphism $\bar{\varphi} : H \longrightarrow A$ such that $\alpha\bar{\varphi} = \varphi$. This will prove two things. First, that $d(H) = \mathfrak{m}$ (for if B is a finite simple quotient of H, then A can be chosen to be a direct product of $\mathfrak{m}$ copies of B). And second, that H is free pro-$\mathcal{C}$ of rank $\mathfrak{m}$ (see Theorem 3.5.9).

Our strategy to find $\bar{\varphi}$ is to search for a convenient open subnormal subgroup U (hence free pro-$\mathcal{C}$ of rank $\mathfrak{m}$) of F, containing H so that φ can be extended to an epimorphism from U onto B; then use the freeness of U to lift that epimorphism to an epimorphism from U onto A; and finally, make sure that the restriction of the latter epimorphism restricted to H is still an epimorphism onto A.

By Lemma 3.5.4, we may assume that in diagram (2), the kernel N is finite. Hence, there exists an open normal subgroup W of A such that $W \cap N = 1$. Consider the commutative diagram



where β, γ, δ are the natural epimorphisms, and $\omega = \gamma\varphi$.

Let $K = \mathrm{Ker}(\omega)$; then K is open in H. By Lemma 8.3.8, there exists an open subnormal subgroup U of F containing H and a continuous epimorphism $U \longrightarrow H/K$ whose restriction to H is the canonical map $H \longrightarrow H/K$. Hence there exists an epimorphism

$$\omega_1 : U \longrightarrow H/K \overset{\cong}{\longrightarrow} A/NW$$

whose restriction to H is ω. Note that $\mathrm{Ker}(\varphi) \leq \mathrm{Ker}(\omega) = K$. Since U is open and subnormal in F, it is a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}$, since $\mathfrak{m}$ is infinite (see Corollary 3.6.4).

Our next step is to construct a special continuous epimorphism

$$\psi_1 : U \longrightarrow A/W$$

lifting ω_1. Say X is a basis of U converging to 1. We know that $H/\mathrm{Ker}(\varphi) \cong B$, $w_0(B) < \mathfrak{m}$ and $w_0(U/H) < \mathfrak{m}$ (the latter inequality is a consequence of our hypothesis $w_0(F/H) < \mathfrak{m}$). Therefore, there exist collections

$$\{V_i^{(1)} \mid V_i^{(1)} \leq_o U, i \in I_1\} \quad \text{and} \quad \{V_i^{(2)} \mid V_i^{(2)} \leq_o U, i \in I_2\}$$

such that $|I_1|, |I_2| < \mathfrak{m}$, $\bigcap_{i \in I_1} V_i^{(1)} = H$ and $\bigcap_{i \in I_2} V_i^{(2)} \cap H = \mathrm{Ker}(\varphi)$ (see Proposition 2.1.4). So, there exists a collection

$$\{V_i \mid V_i \leq_o U, i \in I\}$$

such that $|I| < \mathfrak{m}$ and $\bigcap_{i\in I} V_i = \mathrm{Ker}(\varphi)$. Therefore

$$|X - \mathrm{Ker}(\varphi)| = \left|\bigcup_{i\in I}(X - V_i)\right| < \mathfrak{m},$$

since each $X - V_i$ is a finite set. Hence $|X \cap \mathrm{Ker}(\varphi)| = \mathfrak{m}$. Define a mapping

$$\psi_1 : X \longrightarrow A/W$$

as follows: On $X - \mathrm{Ker}(\varphi)$, let ψ_1 be equal to the function $\sigma\omega_1$, where $\sigma : A/NW \longrightarrow A/W$ is a section of δ; and let ψ_1 on $X \cap \mathrm{Ker}(\varphi)$ be a mapping from $X \cap \mathrm{Ker}(\varphi)$ onto $\mathrm{Ker}(\delta)$ converging to 1 (such a mapping exists since $\mathfrak{m}$ is an infinite set and $\mathrm{Ker}(\delta)$ is finite). Then ψ_1 is a mapping converging to 1 and $\psi_1(X)$ generates A/W. Hence it defines an epimorphism $\psi_1 : U \longrightarrow A/W$, such that $\delta\psi_1 = \omega_1$.

Define $\psi : H \longrightarrow A/W$ as the restriction of ψ_1 to H. Then $\psi(\mathrm{Ker}(\varphi)) = \mathrm{Ker}(\delta)$. One deduces that ψ is onto and $\mathrm{Ker}(\omega) = \mathrm{Ker}(\varphi)\mathrm{Ker}(\psi)$. Next note that

$$\begin{array}{ccc} A & \xrightarrow{\ \alpha\ } & B = A/N \\ \Big\downarrow{\scriptstyle\beta} & & \Big\downarrow{\scriptstyle\gamma} \\ A/W & \xrightarrow{\ \delta\ } & A/NW \end{array}$$

is a pullback diagram since $W \cap N = 1$ (see Exercise 2.10.1). Therefore, ψ and φ induce a homomorphism $\bar{\varphi} : H \longrightarrow A$ such that $\beta\bar{\varphi} = \psi$ and $\alpha\bar{\varphi} = \varphi$. Finally observe that $\bar{\varphi}$ is onto by Lemma 2.10.2. Thus $\bar{\varphi}$ is the desired solution of the $\mathcal{E}$-embedding problem (2).

(b) Suppose first that $\mathfrak{m} > \aleph_0$. Then, $w_0(F/H) = \max\{\aleph_0, d(F/H)\}$. Hence $w_0(F/H) < \mathfrak{m}$, and so the result follows in this case from part (a) above.

Hence we may assume from now on that $\mathfrak{m} \le \aleph_0$. We distinguish two cases.

Case 1. $\mathfrak{m} = n$ is finite.

Observe that $w_0(H) = \aleph_0$, since H is an infinite group. As in case (a), we shall prove that every $\mathcal{E}$-embedding problem (2), where the row is an exact sequence of pro-$\mathcal{C}$ groups with $w_0(A) \le \aleph_0$ and where B is finite, is solvable. Again, this will show both that $d(H) = \aleph_0$ and that H is free of rank $\aleph_0$. By Lemma 3.5.4 we may assume that N and A are finite as well.

Let $K = \mathrm{Ker}(\varphi)$; then K is open in H. By Lemma 8.3.8, there exist an open normal subgroup L of F containing H and a continuous epimorphism $\rho : L \longrightarrow H/K$ extending the map $H \longrightarrow H/K$. In addition, if we put $V = \mathrm{Ker}(\rho)$, then $L/K = H/K \times V/K$. Define an epimorphism $\theta : L \longrightarrow B \times V/K$ as the composition

$$\theta : L \longrightarrow L/K = H/K \times V/K \longrightarrow B \times V/K$$

(the last map is the natural isomorphism induced by φ).

By Theorem 3.6.2, L is a free pro-$\mathcal{C}$ group of finite rank. Next we shall show that, after changing L appropriately if necessary, we can find a basis X of L such that $|X \cap \mathrm{Ker}(\theta)| \geq d(N)$. First remark that as a consequence of Corollary 3.6.4 and our hypothesis,

$$d(L/H) \leq 1 + [F : L](d(F/H) - 1) < 1 + [F : L](\mathrm{rank}(F) - 1) = \mathrm{rank}(L).$$

Hence by Lemmas 8.4.1 and 8.3.8, L can be chosen so that

$$\mathrm{rank}(L) \geq d(L/H) + d(B) + d(N).$$

Put $r = \mathrm{rank}(L)$ and $t = d(B \times V/K)$. Therefore,

$$r = \mathrm{rank}(L) \geq d(B \times V/K) + d(N) = t + d(N).$$

By Proposition 2.5.4, there exists a set of generators

$$X = \{x_1, \ldots, x_t, x_{t+1}, \ldots, x_r\}$$

of L such that $\theta(\langle x_1, \ldots, x_t \rangle) = B \times V/K$ and $\theta(x_i) = 1$ for $i = t+1, \ldots, r$. Since L is a free pro-$\mathcal{C}$ group of rank r, we have that X is a basis of L (see Lemma 3.3.5).

Now, let $\sigma : B \longrightarrow A$ be a section of $\alpha : A \longrightarrow B$. Denote by θ_1 the composition map $L \xrightarrow{\theta} B \times V/K \longrightarrow B$. To define a homomorphism

$$\bar{\theta}_1 : L \longrightarrow A$$

it suffices to define it on X. We do this as follows: $\bar{\theta}_1(x_i) = \sigma\theta_1(x_i)$, for $i = 1, \ldots, t$, and we let $\bar{\theta}_1$ send $x_{t+1}, \ldots, x_r$ to a set of generators of N. This is possible since $r - t \geq d(N)$.

Clearly $\bar{\theta}_1$ is an epimorphism and $\alpha\bar{\theta}_1 = \theta_1$. Let $\bar{\varphi} : H \longrightarrow A$ be the restriction of $\bar{\theta}_1$ to H. Then

$$\alpha\bar{\varphi} = \varphi.$$

Therefore, $\bar{\varphi}(H)N = A$. Finally, remark that $N \leq \bar{\varphi}(H)$ since $x_{t+1}, \ldots, x_r \in \mathrm{Ker}(\theta) = H$. So, $\bar{\varphi}(H) = A$. Thus $\bar{\varphi}$ is an epimorphism, as needed.

Case 2. $\mathfrak{m} = \aleph_0$.

In this case $d(F/H)$ is finite by assumption. We shall prove that every embedding problem (2) with A and B finite is solvable. Again, this will show that H is a free pro-$\mathcal{C}$ group of rank $\aleph_0$.

Write

$$F = \varprojlim F_i,$$

where each F_i is a free pro-$\mathcal{C}$ group of finite rank i and where the canonical map $\pi_i : F \longrightarrow F_i$ is an epimorphism, for each $i = 1, 2, \dots$ (see Corollary 3.3.10). Set $H_i = \pi_i(H)$. Then $H_i \triangleleft F_i$ and

$$F/H = \varprojlim F_i/H_i.$$

Clearly $d(F_i/H_i) \leq d(F/H)$, for $i = 1, 2, \dots$. Choose a natural number n such that $n \geq d(F/H)$ and such that φ factors through H_n (see Lemma 1.1.16). Say $\varphi(h) = \varphi_n\pi_n(h)$, for all $h \in H$, where $\varphi_n : H_n \longrightarrow B$ is an epimorphism. By Case 1, there exists a continuous epimorphism $\bar{\varphi}_n : H \longrightarrow A$ with $\alpha\bar{\varphi}_n = \varphi_n$. Then the composition

$$\bar{\varphi} : H \longrightarrow H_n \xrightarrow{\bar{\varphi}_n} A$$

is the desired solution of the embedding problem (2). □

Part (a) of the result above has an analog valid not only for accessible subgroups, but also for closed subgroups in general, if the class $\mathcal{C}$ is an extension closed variety, in particular for closed subgroups of free profinite groups. Precisely, we have,

Theorem 8.4.3 *Let $\mathcal{C}$ be an extension closed variety of finite groups. Let H be a closed subgroup (not necessarily accessible) of infinite index of a free pro-$\mathcal{C}$ group F of rank $\mathfrak{m} \geq 2$. If $w_0(F/H) < \mathfrak{m}$, then H is also free pro-$\mathcal{C}$ of rank $\mathfrak{m}^*$.*

The proof of this result can be obtained by mimicking almost word by word the proof of part (a) in the theorem above. One simply has to use the result contained in Exercise 8.3.9 rather than Lemma 8.3.8.

Let r be a natural number and let G be a profinite group with $d(G) = r$. We say that G *satisfies Schreier's formula* or that G *is r-freely indexed* if for every open normal subgroup U of G one has

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

The prototype of a group that satisfies Schreier's formula is a free profinite group of rank r (see Theorem 3.6.2).

Corollary 8.4.4 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $r \geq 2$ be a natural number, F a free pro-$\mathcal{C}$ group of rank r, and let H be a closed normal subgroup of F of infinite index. If F/H does not satisfy Schreier's formula, then H is a free pro-$\mathcal{C}$ group of rank $\aleph_0$.*

Proof. Observe that F/H does not satisfy Schreier's formula if and only if there exists some open normal subgroup L of F containing H such that

$$\mathrm{d}(L/H) < 1 + [G : L](r - 1).$$

By Theorem 3.6.2, $\mathrm{d}(L) = 1 + [G : L](r - 1)$, and so $\mathrm{d}(L/H) < \mathrm{d}(L)$. Thus the result follows then from Theorem 8.4.2(b) applied to H and L. □

The following result provides examples of groups which do not satisfy Schreier's formula.

Lemma 8.4.5 *Let $K = K_1 \times K_2$ be a nontrivial direct product decomposition of a profinite group K. Assume that $2 \le d(K) < \infty$. Then K does not satisfy Schreier's formula.*

Proof. Note that $\max\{d(K_1), d(K_2)\} \le d(K) \le d(K_1) + d(K_2)$ $(i = 1, 2)$. If K_i is finite, then K_{3-i} is a proper open normal subgroup of K with $d(K_{3-i}) \le d(K)$ $(i = 1, 2)$. Thus K does not satisfy Schreier's formula. Assume now that both K_1 and K_2 are infinite. Let L_i be a proper open normal subgroup of K_i of index n_i $(i = 1, 2)$. Then $d(L_i) \le 1 + n_i(d(K_i) - 1)$ (see Corollary 3.6.3). So,

$$d(L_1 \times L_2) \le 2 + n_1(d(K_1) - 1) + n_2(d(K_2) - 1) \le 2 + (n_1 + n_2)(d(K) - 1).$$

Next observe that

$$2 + (n_1 + n_2)(d(K) - 1) < 1 + n_1 n_2(d(K) - 1)$$

if

$$n_1 n_2 - (n_1 + n_2) \ge 2,$$

in particular, if $n_1, n_2 \ge 3$. Hence, in any such a case,

$$d(L_1 \times L_2) < 1 + n_1 n_2(d(K) - 1).$$

□

Exercise 8.4.6

(a) Let G be a free pronilpotent group with $d(G) \ge 2$. Show that G does not satisfy Schreier's formula.
(b) Let G be a free prosupersolvable group with $d(G) \ge 2$, and assume that the order of G is divisible by only finitely many primes. Show that G does not satisfy Schreier's formula. (Hint: use Proposition 2.8.11.)

Theorem 8.4.7 *Let p be a prime number and let G be a finitely generated pro-p group. Then G is free pro-p if and only if it satisfies Schreier's formula.*

Proof. Let $d(G) = r$ and let F be the free pro-p group of rank r. If $G = F$, then G satisfies Schreier's formula by Theorem 3.6.2.

Assume that G satisfies Schreier's formula. Let $\varphi : F \longrightarrow G$ be a continuous epimorphism. Consider the Frattini series

$$F = F_1 \ge F_2 \ge \cdots \ge F_i \ge \cdots \quad \text{and} \quad G = G_1 \ge G_2 \ge \cdots \ge G_i \ge \cdots$$

of F and G respectively (that is, F_{i+1} and G_{i+1} are the Frattini subgroups of F_i and G_i respectively, for $i = 1, 2, \ldots$). By Proposition 2.8.13,

$$\bigcap_{i=1}^{\infty} F_i = 1 \quad \text{and} \quad \bigcap_{i=1}^{\infty} G_i = 1;$$

so

$$F = \varprojlim F/F_i \quad \text{and} \quad G = \varprojlim G/G_i.$$

Therefore, it suffices to show that the natural epimorphisms

$$\varphi_i : F/F_i \longrightarrow G/G_i$$

induced by φ are isomorphisms. We do this by induction. This is obviously the case for $i = 1$. Assume that $\varphi_n : F/F_n \longrightarrow G/G_n$ is an isomorphism, and consider the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F_n/F_{n+1} & \longrightarrow & F/F_{n+1} & \longrightarrow & F/F_n & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \psi_{n+1}} & & \downarrow{\scriptstyle \varphi_{n+1}} & & \downarrow{\scriptstyle \varphi_n} & & \\ 1 & \longrightarrow & G_n/G_{n+1} & \longrightarrow & G/G_{n+1} & \longrightarrow & G/G_n & \longrightarrow & 1 \end{array}$$

where ψ_{n+1} is the natural epimorphism induced by φ. Since F and G satisfy Schreier's formula, $d(F_n) = d(G_n)$. Hence the finite $\mathbf{F}_p$-vector spaces F_n/F_{n+1} and G_n/G_{n+1} are isomorphic. Therefore, ψ_{n+1} is an isomorphism. We deduce then from the above diagram and the induction hypothesis that φ_{n+1} is an isomorphism. □

8.5 Homogeneous Pro-$\mathcal{C}$ Groups

The main purpose of this section is to obtain a workable characterization of accessible subgroups of infinite index of free pro-$\mathcal{C}$ groups; this characterization provides criteria to decide which of those accessible subgroups are free pro-$\mathcal{C}$. If $\mathcal{C}$ consists of finite p-groups for a fixed prime number p, then we already have a good understanding of the subgroups of free pro-p groups (see Section 7.7); therefore, for most results in this section we exclude the case of pro-p groups by assuming that the class $\mathcal{C}$ involves at least two primes. Indeed, many of the results in this section are not valid for pro-p groups.

As we saw in Lemma 7.6.3, every projective group G is a subgroup of a free profinite group and by Proposition 7.6.9, such a group is determined by its Frattini quotient $G/\Phi(G)$. However, for many projective groups the Frattini subgroup $\Phi(G)$ is trivial and so $G = G/\Phi(G)$.

The situation is much better when we consider accessible (in particular, normal) subgroups of free profinite groups. The key point in this situation is the replacement of the Frattini subgroup by its analog $M(G)$, the intersection of all closed maximal normal subgroups of G.

As we see in this section, the class of accessible subgroups of infinite index in free profinite groups coincides with the class of 'homogeneous' groups. These are defined as profinite groups having the strong lifting property with respect to certain types of epimorphisms. We remark that, in analogy with projective groups, every homogeneous group is determined uniquely by its local weight and the quotient group $G/M(G)$ (see Theorem 8.5.2 below).

Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups. Denote by $\mathcal{L}$ the class of epimorphisms of pro-$\mathcal{C}$ groups $\alpha : A \longrightarrow B$ such that $\mathrm{Ker}(\alpha) \leq M(A)$. Obviously, $\mathcal{L}$ is an admissible class of epimorphisms (see Definition 3.5.1(c)). An infinite pro-$\mathcal{C}$ group G is said to be *homogeneous* if it has the strong lifting property over the class $\mathcal{L}$.

Remark 8.5.1 By Theorem 3.5.8, a free pro-$\mathcal{C}$ group F of infinite rank is homogeneous.

Let H be a profinite group. Denote by $r_*(H)$ the function that assigns to every finite simple group S the S-rank $r_S(H)$ of H. We shall name it the *S-rank function of H*.

Next we state the main results of this section. The proofs will be given later. The first theorem says that homogeneous groups are characterized by their rank functions and their local weights.

Theorem 8.5.2 *Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups. Let G_1 and G_2 be homogeneous pro-$\mathcal{C}$ groups with $w_0(G_1) = w_0(G_2)$. Then $G_1 \cong G_2$ if and only if $r_*(G_1) = r_*(G_2)$, or equivalently, if and only if $G_1/M(G_1) \cong G_2/M(G_2)$. In particular, a homogeneous pro-$\mathcal{C}$ group G is free pro-$\mathcal{C}$ of infinite rank $\mathfrak{m}$ if and only if $r_S(G) = \mathfrak{m}$ for every simple group $S \in \mathcal{C}$.*

The next result is of a more technical nature; it serves as a preparation for Theorem 8.5.4 which characterizes homogeneous pro-$\mathcal{C}$ groups as accessible groups of infinite index in nonabelian free pro-$\mathcal{C}$ groups.

Theorem 8.5.3 *Assume that $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers. Let $\mathfrak{m}$ be an infinite cardinal and let f be a function that assigns to each simple group $S \in \mathcal{C}$ a cardinal $f(S)$, with $f(S) \leq \mathfrak{m}$. Then there exists a homogeneous pro-$\mathcal{C}$ group G such that $w_0(G) = \mathfrak{m}$ and $r_*(G) = f$.*

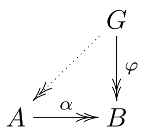
Theorem 8.5.4 *Assume that $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers. Let $F(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Put $\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$. Then, a pro-$\mathcal{C}$ group G is isomorphic to an accessible subgroup of infinite index of $F(\mathfrak{m})$ if and only if G is homogeneous and $w_0(G) = \mathfrak{m}^*$.*

Theorems 8.5.2 and 8.5.4 allow us to classify accessible subgroups of free pro-$\mathcal{C}$ groups. We state this in the following corollary.

Corollary 8.5.5 *Assume that $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers. Let G_1 and G_2 be accessible subgroups of infinite index in a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Then $G_1 \cong G_2$ if and only if $r_*(G_1) = r_*(G_2)$.*

Our strategy to prove these theorems will be as follows. First we prove Theorem 8.5.2. Then we prove that homogeneous groups are precisely the accessible subgroups of free pro-$\mathcal{C}$ groups (of infinite index if the rank of the free group is finite). Finally we shall show Theorem 8.5.3.

Lemma 8.5.6 *Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups. Let G be a pro-$\mathcal{C}$ homogeneous group with $w_0(G) = \mathfrak{m}$. Then any embedding problem*


(3)

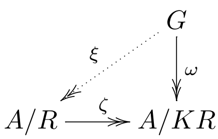
with $w_0(A) \leq \mathfrak{m}$, $\mathrm{Ker}(\alpha) \leq M(A)$ and $w_0(M(A)/\mathrm{Ker}(\alpha)) < \mathfrak{m}$, is solvable.

Proof. We consider two cases.

Case 1. $K = \mathrm{Ker}(\alpha)$ is a finite minimal normal subgroup of A.

From the finiteness of $K = \mathrm{Ker}(\alpha)$ it follows that $w_0(M(A)) < \mathfrak{m}$. Then, by Lemma 8.3.8, there exists a closed normal subgroup L of A containing $M(A)$ and a continuous epimorphism $\rho : L \longrightarrow M(A)$ such that ρ is the identity map on $M(A)$ and $w_0(A/L) \leq w_0(M(A)) < \mathfrak{m}$; moreover $R = \mathrm{Ker}(\rho)$ is normal in A and $RM(A) = A$. Clearly $R \cap M(A) = 1$ and so $w_0(L/R) = w_0(M(A))$. Therefore, $w_0(A/R) < \mathfrak{m}$, since $\mathfrak{m}$ is infinite.

Consider the embedding problem

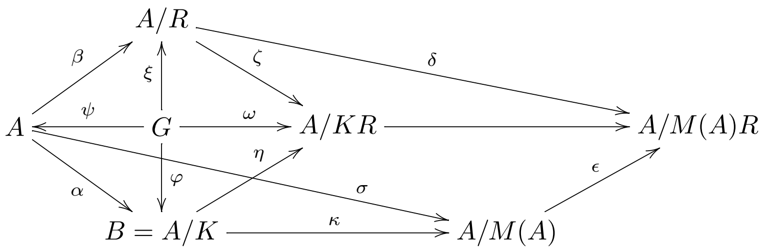


where ζ is the canonical epimorphism and ω is the composition of natural epimorphisms $G \xrightarrow{\varphi} B = A/K \xrightarrow{\eta} A/KR$. Clearly $w_0(A/KR) < \mathfrak{m}$ and $\mathrm{Ker}(\zeta) = KR/R \leq M(A/R)$ (since $K \leq M(A)$). Hence there exists an epimorphism ξ solving the embedding problem above, i.e., such that $\omega = \zeta\xi$.

Next we define a map $\psi : G \longrightarrow A$; to do this observe that the commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\beta} & A/R \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\zeta} \\ A/K & \xrightarrow{\eta} & A/KR \end{array}$$

is a pullback since $K \leq M(A)$ and $R \cap M(A) = 1$ (see Exercise 2.10.1). Therefore, from $\eta\varphi = \zeta\xi$, we deduce the existence of a continuous homomorphism $\psi : G \longrightarrow A$ such that $\alpha\psi = \varphi$ and $\beta\psi = \xi$. It remains to prove that ψ is surjective. Next consider the following commutative diagram



where all mappings are (canonical) epimorphisms except possibly ψ.

Note that

$$\begin{array}{ccc} A & \xrightarrow{\beta} & A/R \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\delta} \\ A/M(A) & \xrightarrow{\epsilon} & A/M(A)R \end{array}$$

is a pullback diagram since $R \cap M(A) = 1$. Observe that ψ is also the map induced by the pair ξ and $\kappa\varphi$ with respect to this pullback. According to Lemma 2.10.2, to prove that ψ is surjective, it suffices to show that

$$\mathrm{Ker}(\xi)\mathrm{Ker}(\kappa\varphi) = \mathrm{Ker}(\delta\xi).$$

Since $A/M(A) \cong G/\mathrm{Ker}(\kappa\varphi)$, one has that $\mathrm{Ker}(\kappa\varphi)$ is the intersection of maximal normal subgroups of G; hence $\mathrm{Ker}(\kappa\varphi) \geq M(G)$. Thus, using this and Lemma 8.3.7, we have

$$\mathrm{Ker}(\delta\xi) = \xi^{-1}(M(A)R/R) = \mathrm{Ker}(\xi)M(G) \leq \mathrm{Ker}(\xi)\mathrm{Ker}(\kappa\varphi).$$

To prove equality observe that

$$\delta\xi(\mathrm{Ker}(\xi)\mathrm{Ker}(\kappa\varphi)) = \delta\xi(\mathrm{Ker}(\kappa\varphi)) = \epsilon\kappa\varphi(\mathrm{Ker}(\kappa\varphi)) = 1.$$

Case 2. General $K = \mathrm{Ker}(\alpha)$.

By Corollary 2.6.5, there exist an ordinal number μ and a chain of closed subgroups of K

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

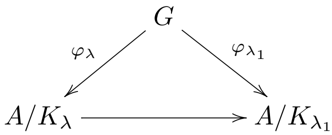
such that

(i) each K_λ is a normal subgroup of A with $K_\lambda/K_{\lambda+1} \in \mathcal{C}$; moreover K_λ is maximal with respect to these properties;
(ii) if λ is a limit ordinal, $K_\lambda = \bigcap_{\nu<\lambda} K_\nu$; and
(iii) if K is an infinite group, then $w_0(M(A)/K_\lambda) < w_0(A)$ whenever $\lambda < \mu$.

We use induction (transfinite, if K is infinite) on λ to construct an epimorphism

$$\varphi_\lambda : G \longrightarrow A/K_\lambda$$

for each $\lambda \le \mu$, such that if $\lambda_1 \le \lambda$ the diagram



commutes, where the horizontal mapping is the natural epimorphism. Then $\varphi_\mu : G \longrightarrow A$ will be a solution to the embedding problem (3).

Note that $A/K_0 = B$; so, put $\varphi_0 = \varphi$. Let $\lambda \le \mu$ and assume that φ_ν has been defined for all $\nu < \lambda$ so that the above conditions are satisfied.

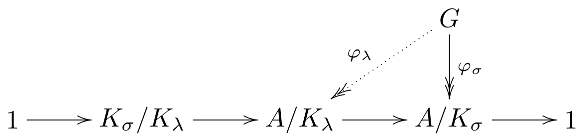
If λ is a limit ordinal, then

$$A/K_\lambda = \varprojlim_{\nu<\lambda} A/K_\nu;$$

in this case, define

$$\varphi_\lambda = \varprojlim_{\nu<\lambda} \varphi_\nu.$$

If, on the other hand, $\lambda = \sigma + 1$, we define φ_λ to be a solution to the embedding problem



Remark that such a solution exists because $\mathrm{Ker}(A/K_\lambda \longrightarrow A/K_\sigma) = K_\sigma/K_\lambda \le M(A/K_\lambda) = M(A)/K_\lambda$ and

$$w_0((M(A)/K_\lambda)/(K_\sigma/K_\lambda)) = w_0(M(A)/K_\lambda) < \mathfrak{m}.$$

It is clear that in either case φ_λ satisfies the required conditions. □

The following proposition is a variation of Proposition 3.5.6.

Proposition 8.5.7 *Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups. Let $\mathfrak{m}$ be an infinite cardinal and let G_1 and G_2 be homogeneous pro-$\mathcal{C}$ groups such that $w_0(G_1) = w_0(G_2) = \mathfrak{m}$. Assume that N_i is a normal subgroup of G_i such that $N_i \le M(G_i)$ and $w_0(M(G_i)/N_i) < \mathfrak{m}$ $(i = 1, 2)$. Then any isomorphism $\beta : G_1/N_1 \longrightarrow G_2/N_2$ can be lifted to an isomorphism $\omega : G_1 \longrightarrow G_2$.*

Proof. Let μ be the smallest ordinal whose cardinal is $\mathfrak{m}$. By Corollary 2.6.5, there exists a chain of closed normal subgroups of G_i $(i = 1, 2)$

$$N_i = N_{i0} \geq N_{i1} \geq \cdots \geq N_{i\lambda} \geq \cdots \geq N_{i\mu} = 1$$

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

(1) $N_{i\lambda}/N_{i\lambda+1}$ is finite for $\lambda \geq 0$,
(2) if λ is a limit ordinal, $N_{i\lambda} = \bigcap_{\nu<\lambda} N_{i\nu}$, and
(3) $w_0(M(G_i)/N_{i\lambda}) < \mathfrak{m}$, if $\lambda < \mu$.

One now proceeds essentially as in the proof of Proposition 3.5.6; the only new ingredient is the use of Lemma 8.5.6 at the appropriate places. We omit the details. □

Proof of Theorem 8.5.2. Since $G/M(G) \cong \prod_{S\in\Sigma_\mathcal{C}} \prod_{r_S(G)} S$ for any pro-$\mathcal{C}$ group G, the equality $r_*(G_1) = r_*(G_2)$ implies the existence of an isomorphism $\beta : G_1/M(G_1) \longrightarrow G_2/M(G_2)$. In light of Proposition 8.5.7, β lifts to an isomorphism $G_1 \longrightarrow G_2$.

For the last statement of the theorem, just recall that if F is a free pro-$\mathcal{C}$ group of infinite rank $\mathfrak{m}$, then $r_S(F) = \mathfrak{m}$ for each finite simple group $S \in \mathcal{C}$ (see Proposition 8.2.6). □

Next we construct certain groups of arbitrarily large local weight which we shall need in several occasions.

Lemma 8.5.8 *Let S, T be finite simple groups with $S \ncong T$ if $S = C_p$, where p is a prime number. Then, for every cardinal number $\mathfrak{m}$, there exists a profinite group $A = A_\mathfrak{m}(S, T)$ such that*

(1) *A has a unique maximal closed normal subgroup B and $A/B \cong T$;*
(2) *$B = \prod_{i\in I} B_i$, where $|I| = \mathfrak{m}$ and B_i is a finite direct product of copies of S.*

Proof. Let I be an indexing set of cardinality $\mathfrak{m}$. For each $i \in I$, define a group B_i as follows. If S is nonabelian, put

$$B_i = \prod_{t\in T} S_t,$$

where S_t is a copy of S. And if $S = C_p$, choose

$$B_i = L = \mathbf{F}_p \oplus \cdots \oplus \mathbf{F}_p$$

to be a fixed irreducible T-module of dimension $n > 1$ over $\mathbf{F}_p$.

Let

$$B = \prod_{i\in I} B_i.$$

If S is nonabelian, let an action of T on B_i be defined by

$$(s_t)^{t_1} = (s_{tt_1}) \quad (t, t_1 \in T; (s_t) \in B_i).$$

And if $S = C_p$, let the action of T on B_i be the module action. Let T act on B via the action on each B_i described above.

Consider the corresponding semidirect product

$$A = B \rtimes T.$$

Since the action of T on B is continuous, A is a profinite group. In fact, each B_i $(i \in I)$ is T-invariant under this action, and so $B_i \triangleleft A$ for each $i \in I$.

Clearly B is a maximal closed normal subgroup of A. We claim that B is the unique maximal closed normal subgroup of A. Indeed, let K be a maximal closed normal subgroup of A, and suppose $K \not\leq B$. Then there exists some $j \in I$ with $B_j \not\leq K$, that is, $B_j \cap K \neq B_j$. Since K is maximal normal, one has that $A = B_j K$. Plainly $B_j \cap K \triangleleft A$. Note that B_i does not contain any proper nontrivial T-invariant subgroup; hence, $B_j \cap K = 1$. Therefore,

$$A/K \cong B_j/B_j \cap K \cong B_j.$$

But B_j is not simple; therefore, K is not maximal normal, a contradiction. Thus B is the unique maximal closed normal subgroup of A, as asserted. □

Corollary 8.5.9 *Assume that $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers. Then every homogeneous pro-$\mathcal{C}$ group G is infinitely generated.*

Proof. By definition of homogeneous group, $w_0(G) = \mathfrak{m}$ is infinite. Let $S, T \in \mathcal{C}$ be simple groups (different if S is abelian). Construct $A = A_{\mathfrak{m}}(S, T)$ as in Lemma 8.5.8. Clearly $d(A) = w_0(A) = \mathfrak{m}$. Consider the embedding problem

$$\begin{array}{ccc} & & G \\ & \swarrow^{\bar\varphi} & \downarrow{\scriptstyle\varphi} \\ A & \xrightarrow{\alpha} & S \end{array}$$

where α is the natural epimorphism $A = B \rtimes S \longrightarrow S$. Then $\mathrm{Ker}(\alpha) = M(A) = B$. Hence there exists an epimorphism $\bar\varphi : G \longrightarrow A$ such that $\alpha\bar\varphi = \varphi$. Thus $d(G) \geq d(A) = w_0(G)$. Therefore, $d(G) = w_0(G)$. □

Proposition 8.5.10 *Assume that $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers. Let H be an accessible subgroup of a free pro-$\mathcal{C}$ group $F = F_{\mathcal{C}}(\mathfrak{m})$, where $\mathfrak{m} \geq 2$. Assume that H is nontrivial and has infinite index in F. Then H is a homogeneous pro-$\mathcal{C}$ group and $w_0(H) = \mathfrak{m}^*$, where $\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$.*

Proof. Consider an embedding problem of pro-$\mathcal{C}$ groups

$$\begin{array}{ccc} & & H \\ & \swarrow^{\bar\varphi} & \downarrow \varphi \\ A & \xrightarrow{\alpha} & B \end{array}$$

where $\mathrm{Ker}(\alpha) \leq M(A)$, α and φ are epimorphisms, $w_0(A) \leq \mathfrak{m}^*$ and $w_0(B) < \mathfrak{m}^*$. We must prove that there exists an epimorphism $\bar\varphi : H \longrightarrow A$ such that $\alpha\bar\varphi = \varphi$ and that $w_0(H) = \mathfrak{m}^*$. By Lemma 3.5.4, we may assume that $\mathrm{Ker}(\alpha)$ is a finite minimal normal subgroup of A.

Step 1. We shall first show the existence of an epimorphism $\bar\varphi : H \longrightarrow A$ such that $\alpha\bar\varphi = \varphi$. (Observe that this will not yet show that H is homogeneous, for one does not know that $w_0(H) = \mathfrak{m}^*$; this will be proved in Step 2.) By Lemma 8.3.8, there exists an accessible subgroup L of F containing H and a continuous epimorphism $\rho : L \longrightarrow H/\mathrm{Ker}(\varphi)$ such that

$$w_0(F/L) \leq w_0(H/\mathrm{Ker}(\varphi)) = w_0(B) < \mathfrak{m}^*$$

and such that the restriction of ρ to H is the natural map $H \longrightarrow H/\mathrm{Ker}(\varphi)$. Define an epimorphism

$$\varphi_1 : L \longrightarrow B$$

to be the composition of epimorphisms $L \xrightarrow{\rho} H/\mathrm{Ker}(\varphi) \longrightarrow B$, the latter map being the isomorphism induced by φ. Plainly φ is the restriction of φ_1 to H.

If $\mathfrak{m}$ is finite, then $\mathfrak{m}^* = \aleph_0$; hence B is finite. Therefore, A and F/L are finite. In addition L can be chosen subnormal in F so that $[F : L]$ is arbitrarily large (see Lemma 8.3.8); thus L is a free pro-$\mathcal{C}$ group whose rank is finite, but as large as we wish (see Corollary 3.6.4). Choose L to be such that $\mathrm{rank}(L) \geq d(A)$.

If $\mathfrak{m} \geq \aleph_0$, then L is free pro-$\mathcal{C}$ of rank $\mathfrak{m}$; indeed, if $[F : L]$ is finite, this follows from Theorem 3.6.2; while if $[F : L]$ is infinite, it follows from Theorem 8.4.2, since then $w_0(F/L) < \mathfrak{m}^* = \mathfrak{m}$.

Next consider the embedding problem

$$\begin{array}{ccc} & & L \\ & \swarrow^{\psi} & \downarrow \varphi_1 \\ A & \xrightarrow{\alpha} & B \end{array}$$

By Theorem 3.5.8 or Theorem 3.5.9 and the considerations above, φ_1 can be lifted to an epimorphism $\psi : L \longrightarrow A$ such that $\alpha\psi = \varphi_1$. Define $\bar\varphi : H \longrightarrow A$ to be the restriction of ψ to H. It remains to show that $\bar\varphi$ is an epimorphism, that is, $\psi(H) = A$.

From the definition of ψ we deduce that $\alpha\psi(H) = B$. Since $\mathrm{Ker}(\alpha) \leq M(A)$, we have $\psi(H)M(A) = A$. On the other hand, $\psi(H)$ is an accessible subgroup of A (see Proposition 8.3.1); thus by Proposition 8.3.6, we have $\psi(H) = A$, as desired.

Step 2. Next we show that $w_0(H) = \mathfrak{m}^*$. Certainly $w_0(H) \leq \mathfrak{m}^*$. Since H is nontrivial, there exists some finite simple group $T \in \mathcal{C}$ and an epimorphism $\delta : H \longrightarrow T$. Choose a finite simple group $S \in \mathcal{C}$ (if T is abelian, choose $S \not\cong T$). Consider the group $A = A_{\mathfrak{m}^*}(S,T)$ constructed in Lemma 8.5.8; then there exists a canonical epimorphism

$$\beta : A \longrightarrow A/M(A) = T.$$

As shown in Step 1, the embedding problem

$$\begin{array}{ccc} & & H \\ & \overset{\bar\delta}{\swarrow} & \downarrow \delta \\ A = A_{\mathfrak{m}^*}(S,T) & \overset{\beta}{\twoheadrightarrow} & T \end{array}$$

is solvable, since obviously $\mathrm{Ker}(\beta) \leq M(A)$. In other words, there exists an epimorphism $\bar\delta : H \longrightarrow A_{\mathfrak{m}^*}(S,T)$ such that $\beta\bar\delta = \delta$. Thus,

$$w_0(H) \geq w_0(A_{\mathfrak{m}^*}(S,T)) = \mathfrak{m}^*,$$

as desired. $\square$

Proposition 8.5.11 *Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Assume that f is a function that assigns to each finite simple group $S \in \mathcal{C}$ a cardinal number $f(S)$ such that $f(S) \leq \mathfrak{m}^*$. Then there exists an accessible subgroup H of infinite index in F such that $f(S) = r_S(H)$ for every $S \in \Sigma_{\mathcal{C}}$.*

Proof. Let X be a basis of $F_{\mathcal{C}}(\mathfrak{m})$ converging to 1. Choose $x \in X$ and denote by N the closed normal subgroup of F generated by x. By Theorem 8.1.3, N is a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}^*$. Note that the index of N in F is infinite. We shall construct H as an accessible subgroup of N. From the isomorphism $N \cong F_{\mathcal{C}}(\mathfrak{m}^*)$, it follows that

$$N/M(N) \cong \prod_{S \in \Sigma_{\mathcal{C}}} \prod_{\mathfrak{m}^*} S.$$

Since $f(S) \leq \mathfrak{m}^*$ for all $S \in \Sigma_{\mathcal{C}}$, there exists $K \triangleleft_c N/M(N)$ such that

$$K \cong \prod_{S \in \Sigma_{\mathcal{C}}} \prod_{f(S)} S.$$

Let $\varphi : N \longrightarrow N/M(N)$ be the canonical epimorphism. Denote by $\mathcal{L}$ the set of all accessible subgroups L of N such that $\varphi(L) = K$. The set $\mathcal{L}$ is nonempty, since $\varphi^{-1}(K) \in \mathcal{L}$. Define a partial order on $\mathcal{L}$ by reverse inclusion, that is, if $L, L' \in \mathcal{L}$, we define $L \preceq L'$ if and only if $L \geq L'$. We claim that $\mathcal{L}$ is an inductive poset. Let

$$\cdots \geq L_i \geq \cdots \geq L_j \geq \cdots$$

be a chain in $\mathcal{L}$ indexed by I. Put $L = \bigcap_{i \in I} L_i$. Plainly $L \succeq L_i$ for all $i \in I$. By Proposition 2.1.4, $\varphi(L) = K$. In light of Proposition 8.3.5, L is an accessible subgroup of N. Hence $L \in \mathcal{L}$. This proves the claim. By Zorn's lemma, there exists a maximal element H in $(\mathcal{L}, \preceq)$. That is, if $L \in \mathcal{L}$ and $L \leq H$, then $H = L$.

We shall show that $f(S) = r_S(H)$ for all $S \in \Sigma_{\mathcal{C}}$. Let V be an arbitrary maximal closed normal subgroup of N. Then, either $V \geq H$ or $H \cap V$ is a maximal closed normal subgroup of H; hence $V \geq M(H)$; therefore

$$H \cap M(N) \geq M(H).$$

To prove the reverse inclusion, consider a maximal closed normal subgroup W of H. Then, either $W \geq H \cap M(N)$ or $(H \cap M(N))W = H$. In the latter case, $M(N)W = M(N)H$; hence $\varphi(W) = \varphi(H) = K$, contradicting the minimality of H. Therefore, $H \cap M(N) \leq W$. Since W is arbitrary, $M(H) \geq H \cap M(N)$. Thus $H \cap M(N) = M(H)$. This means that $H/M(H) \cong K$. Therefore, $f(S) = r_S(H)$ for all $S \in \Sigma_{\mathcal{C}}$. □

Proof of Theorem 8.5.3. By Proposition 8.5.11, there exists an accessible subgroup G of $F_{\mathcal{C}}(\mathfrak{m})$ of infinite index such that $f(S) = r_S(G)$ for all $S \in \Sigma_{\mathcal{C}}$. The group G is homogeneous and $w_0(G) = \mathfrak{m}$ by Proposition 8.5.10. □

Proof of Theorem 8.5.4. Let G be a homogeneous pro-$\mathcal{C}$ group of local weight $\mathfrak{m}^*$. By Proposition 8.5.11, there exists an accessible subgroup H of $F_{\mathcal{C}}(\mathfrak{m})$ of infinite index such that $r_S(H) = r_S(G)$ for all $S \in \Sigma_{\mathcal{C}}$. By Proposition 8.5.10, H is homogeneous with $w_0(H) = \mathfrak{m}^*$. Hence by Theorem 8.5.2, $H \cong G$. The converse is just the content of Proposition 8.5.10. □

Corollary 8.5.12 *Assume that $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers. Let N be an accessible subgroup of a free pro-$\mathcal{C}$ group $F = F_{\mathcal{C}}(\mathfrak{m})$ of rank $\mathfrak{m} \geq 2$. Then $d(N)$ is finite if and only if $\mathfrak{m}$ is finite and N has finite index in F.*

Proof. If F has finite rank and the index of N in F is finite, then clearly $d(N)$ is finite. Conversely, assume that $d(N)$ is finite. If the index of N in F were infinite, then, by Proposition 8.5.10 N would be homogeneous of rank $\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$. Hence N has finite index and so it is open and subnormal in F. Therefore, by Corollary 3.6.4, $\mathfrak{m}$ has to be finite. □

Now we can prove the following criterion of freeness of an accessible subgroup of a free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(\mathfrak{m})$ of rank $\mathfrak{m} \geq 2$.

Theorem 8.5.13 *Assume that $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers. Let $F = F(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Then, a nontrivial accessible subgroup H of F of infinite index is free pro-$\mathcal{C}$ if and only if $r_S(H) = \mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$ for all $S \in \Sigma_{\mathcal{C}}$.*

Proof. By Theorem 8.5.4, H is homogeneous with $w_0(H) = \mathfrak{m}^*$. By Corollary 8.5.12, $d(H)$ is infinite. Hence $d(H) = \mathfrak{m}^*$. Now, if H is free, then its rank is $\mathfrak{m}^*$ by Corollary 2.6.3. Therefore, $r_S(H) = \mathfrak{m}^*$ for all $S \in \Sigma_{\mathcal{C}}$.

Conversely, if $r_S(H) = \mathfrak{m}^*$ for all $S \in \Sigma_{\mathcal{C}}$, then, by Theorem 8.5.2, $H \cong F_{\mathcal{C}}(\mathfrak{m}^*)$, since both groups are homogeneous and $w_0(H) = w_0(F_{\mathcal{C}}(\mathfrak{m}^*))$. □

An accessible subgroup H of a homogeneous group G is homogeneous of the same local weight as G, according to Theorem 8.5.4. If H is open in G one can get more precise information about H. It is more convenient to state the corresponding result in terms of accessible subgroups of free pro-$\mathcal{C}$ groups.

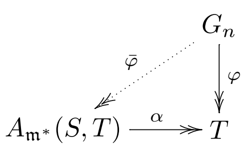
Theorem 8.5.14 *Assume that $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers. Let G be an accessible subgroup of infinite index of a free pro-$\mathcal{C}$ group $F = F_{\mathcal{C}}(\mathfrak{m}), \mathfrak{m} \geq 2$, and let H be a proper open normal subgroup of G. Set $\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$. Then*

(a) $r_S(H) = \mathfrak{m}^*$ *for every nonabelian finite simple group S;*
(b) $r_p(H) = \mathfrak{m}^*$ *if G/H is not a finite p-group (any prime number p);*
(c) $r_p(H) = [G : H](r_p(G) - 1) + 1$ *if G/H is a finite p-group (any prime number p; note that if $r_p(G)$ is infinite, then $[G : H](r_p(G) - 1) + 1 = r_p(G)$ by convention).*

Proof. (a) Let

$$H = G_{n+1} \lhd_c G_n \lhd_c \cdots \lhd_c G_1 \lhd_c G_0 = G$$

be a composition series from H to G. Then $T = G_n/H$ is a simple group. Since S is nonabelian, we can consider the group $A_{\mathfrak{m}^*}(S, T)$ constructed in Lemma 8.5.8. Let $\alpha : A_{\mathfrak{m}^*}(S, T) \longrightarrow T$ and $\varphi : G_n \longrightarrow T$ be the canonical epimorphisms. By Theorem 8.5.4, the group G_n is homogeneous and $w_0(G_n) = \mathfrak{m}^*$. Since $\mathrm{Ker}(\alpha) = M(A_{\mathfrak{m}^*}(S, T))$, the embedding problem



is solvable. Clearly, $\bar{\varphi}(H) = M(A_{\mathfrak{m}^*}(S, T))$, since $M(A_{\mathfrak{m}^*}(S, T))$ is the unique maximal normal subgroup of $M(A_{\mathfrak{m}^*}(S, T)) \cong \prod_{\mathfrak{m}^*} S$. It follows that

$$r_S(H) \geq r_S(M(A_{\mathfrak{m}^*}(S, T)) = \mathfrak{m}^*.$$

On the other hand, it is obvious that $r_S(H) \leq \mathfrak{m}^*$.

(c) Let $R_p(G)$ be the intersection of all normal subgroups K of G such that the quotient G/K is a pro-p group (see Lemma 3.4.1). Since G is projective, the quotient group $G/R_p(G)$ is free pro-p by Proposition 7.7.7. We claim that the rank of $G/R_p(G)$ is $r_p(G)$. To see this, put $L = G/R_p(G)$. Note that $\mathrm{rank}(L) = d(L/\Phi(L))$ and $R_p(G) \leq \overline{[G,G]G^p}$. Hence $\Phi(L) = \overline{[G,G]G^p}/R_p(G)$; so $L/\Phi(L) \cong G/\overline{[G,G]G^p}$. Thus $\mathrm{rank}(L) = d(G/\overline{[G,G]G^p}) = r_p(G)$, proving the claim.

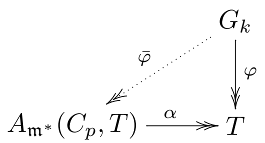
Now, since $G/\overline{[H,H]H^p}$ is an extension of the pro-p group $H/\overline{[H,H]H^p}$ by G/H, then $G/\overline{[H,H]H^p}$ is a pro-p group. Therefore $R_p(G) \leq \overline{[H,H]H^p}$. Let H_0 be the image of H in $G/R_p(G)$, that is, $H_0 = H/R_p(G)$. Hence $\mathrm{rank}(H_0) = [G:H](\mathrm{rank}(G/R_p(G)) - 1) + 1$ (see Theorem 3.6.2). Then the following equalities complete the proof of (c)

$$r_p(H) = r_p(H_0) = \mathrm{rank}(H_0) = [G:H](\mathrm{rank}(G/R_p(G)) - 1) + 1.$$

(b) Assume that $G = G/H$ is not a p-group. Let

$$H = G_{n+1} \lhd_c G_n \lhd_c \cdots \lhd_c G_1 \lhd_c G_0 = G$$

be a composition series. Then there are quotients in this series which are not isomorphic to C_p. Let $0 \leq k \leq n$ be the largest index such that $G_k/G_{k+1} \ncong C_p$. We claim that $r_p(G_{k+1}) = \mathfrak{m}^*$. Put $T = G_k/G_{k+1}$ and consider the group $A_{\mathfrak{m}^*}(C_p, T)$ from Lemma 8.5.8. Then $M(A_{\mathfrak{m}^*}(C_p,T)) \cong \prod_{\mathfrak{m}_0} C_p$. Hence, by Theorem 8.5.4, the embedding problem



is solvable. Since $M(A_{\mathfrak{m}^*}(C_p,T))$ is the unique maximal normal subgroup of $A_{\mathfrak{m}^*}(C_p,T)$, then $\bar{\varphi}(G_{k+1}) = M(A_{\mathfrak{m}^*}(C_p,T)$. Hence $w_0(G_{k+1}) \geq \mathfrak{m}^*$; thus $r_p(G_{k+1}) = \mathfrak{m}^*$.

Since $\mathfrak{m}^*$ is infinite and G_i/G_{i+1} is a finite p-group for all $i = k+1, k+2, \ldots, n$, one deduces from (b) inductively that $r_p(G_{n+1}) = r_p(H) = \mathfrak{m}^*$, as desired. □

Corollary 8.5.15 *Assume that $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers. Let G be an accessible subgroup of a free pro-$\mathcal{C}$ group $F = F_{\mathcal{C}}(\mathfrak{m})$ of rank $\mathfrak{m} \geq 2$. Then G is virtually free pro-$\mathcal{C}$. More precisely, if H is a maximal open normal subgroup of G, then*

(a) *H is free pro-$\mathcal{C}$ if G/H is a finite nonabelian simple group;*
(b) *H contains a free pro-$\mathcal{C}$ subgroup of finite index if $G/H \cong C_p$, for some prime p.*

Proof. We may assume that G has infinite index, for otherwise the result follows from Corollary 3.6.4.

(a) By Theorem 8.5.14, $r_S(H) = \mathfrak{m}^*$ for every finite simple group S. Hence H is free pro-$\mathcal{C}$ of rank $\mathfrak{m}^*$ by Theorem 8.5.13.
(b) Choose a nonabelian finite simple group S. Then $r_S(H) = \mathfrak{m}^*$ by Theorem 8.5.14. In particular, there exists some open normal subgroup K of H with $H/K \cong S$. Then by part (a), K is free pro-$\mathcal{C}$ of rank $\mathfrak{m}^*$. □

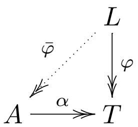
Theorem 8.5.16 *Assume that $\mathcal{C}$ is an extension closed variety of finite groups involving at least two different prime numbers. Let R be a closed finitely generated subgroup of a free pro-$\mathcal{C}$ group $F = F(\mathfrak{m})$ of rank $\mathfrak{m} \geq 2$. Suppose R contains a nontrivial accessible subgroup H of F. Then $\mathfrak{m}$ is finite and R is open in F.*

Proof. First note that if H is open in F, then so is R, and this implies the finiteness of $\mathfrak{m}$ by Theorem 3.6.2. Thus, we may assume that H has infinite index in F. Then, by Theorem 8.5.4, H is homogeneous and $w_0(H) = \mathfrak{m}^*$.

Since H is nontrivial, there exists an epimorphism $H \longrightarrow T$ onto some finite simple group $T \in \mathcal{C}$. Therefore (see Exercise 8.3.9), there exist an open subgroup L of F containing H and a continuous epimorphism $\varphi : L \longrightarrow T$ extending $H \longrightarrow T$. Put $R_1 = R \cap L$. Choose a finite simple group $S \in \mathcal{C}$ such that $S \ncong T$ if T is abelian.

Case 1. $\mathfrak{m}$ is infinite.

If $\mathfrak{m} > \aleph_0$, then $w_0(R) \geq w_0(H) = \mathfrak{m} > \aleph_0$, contradicting the fact that R is finitely generated. Therefore, $\mathfrak{m} = \aleph_0$. Construct $A = A_{\aleph_0}(S, T)$ as in Lemma 8.5.8. Hence, there exists an epimorphism $\alpha : A \longrightarrow T$ whose kernel is $M(A) \cong \prod_{\aleph_0} S$. By Theorem 3.6.2, L is free pro-$\mathcal{C}$ of rank $\aleph_0$; so, the embedding problem



is solvable. Say $\bar{\varphi} : L \longrightarrow A$ is a continuous epimorphism making the diagram commutative. Note that $\bar{\varphi}(H)$ is an accessible subgroup of A. The equality $\alpha(\bar{\varphi}(H)) = \varphi(H) = T$ implies that $\bar{\varphi}(H)M(A) = A$. Then, by Proposition 8.3.6, $\bar{\varphi}(H) = A$. Since $H \leq R_1 \leq L$, we have $\bar{\varphi}(R_1) = A$. Therefore, $d(R_1) \geq d(A) = \aleph_0$. However, R_1 is finitely generated because it is open in R, a contradiction. Thus, subgroups R and L with the stated conditions do not exist if $\mathfrak{m}$ is infinite.

Case 2. $\mathfrak{m}$ is finite.

Since R_1 is open in R, one has that $d(R_1) < \infty$. Choose a natural number n such that $d(A) > d(R_1)$, where $A = A_n(S, T)$ is the group constructed in Lemma 8.5.8.

We may assume that $[F : R_1] = \infty$ (otherwise, R would be of finite index in F as needed). Then there exists an open subgroup V of F such that $R_1 < V \leq L$ and $[F : V] \geq d(A)$. Set $\varphi^* = \varphi_{|V}$. Since $H \leq R_1 < V$, then $\varphi^*(V) = \varphi(V) \geq \varphi(H) = T$. So, φ^* is an epimorphism of V onto T whose restriction to H coincides with $H \longrightarrow T$. By Theorem 3.6.2, V is a free pro-$\mathcal{C}$ group of rank $[F : V](\mathfrak{m} - 1) + 1 > d(A)$. Hence one can extend the epimorphism φ^* to an epimorphism $\bar{\varphi} : V \longrightarrow A$. As in the previous case, it follows that $\bar{\varphi}$ maps R_1 onto A. This, however, contradicts the fact that (by construction) $d(A)$ is greater than $d(R_1)$. □

Exercise 8.5.17 Let $\mathcal{C}$ be an NE-formation of finite groups involving at least two different prime numbers. Let R be an accessible subgroup of a free pro-$\mathcal{C}$ group $F = F(\mathfrak{m})$ of rank $\mathfrak{m} \geq 2$. Suppose that R is finitely generated. Then $\mathfrak{m}$ is finite and R is open in F.

Compare the following lemma with Theorem 3.2.9.

Lemma 8.5.18 *Assume that $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers. Let $F = F(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$ and let G be an accessible subgroup of F with $w_0(G) = \aleph_0$. Suppose that every group in $\mathcal{C}$ is an epimorphic image of G. Then G is a free profinite group of countably infinite rank.*

Proof. By Theorem 8.5.13, it suffices to prove that $r_S(G) = \aleph_0$ for every $S \in \Sigma_{\mathcal{C}}$. For every natural number n and every $S \in \Sigma_{\mathcal{C}}$, there is a epimorphism $G \longrightarrow \prod_n S$. Hence $r_S(G) \geq n$ by Lemma 8.2.5. Since n is arbitrarily large, the result follows. □

Exercise 8.5.19 Let $\{G_i, \varphi_{ij}, I\}$ be a surjective inverse system of countably generated homogeneous pro-$\mathcal{C}$ groups G_i over a countable poset I. Then $G = \varprojlim_{i \in I} G_i$ is a countably generated homogeneous pro-$\mathcal{C}$ group.

8.6 Normal Subgroups

According to Theorem 3.6.2, open normal subgroups of a free pro-$\mathcal{C}$ group are free and their ranks are determined by their indices. By Theorem 8.5.4, closed normal subgroups of a free pro-$\mathcal{C}$ group are homogeneous and therefore they are determined up to isomorphism by their S-rank functions (see Theorem 8.5.2). Thus, to classify normal subgroups of free pro-$\mathcal{C}$ groups it suffices to describe all their possible S-rank functions. These description is contained in Theorems 8.6.11 and 8.6.12.

In Theorem 8.5.13 we saw that if $\mathcal{C}$ involves at least two primes, then $r_S(H) = m^* = \max\{\mathfrak{m}, \aleph_0\}$ for (in particular) any closed normal subgroup H of infinite index in a nonabelian free pro-$\mathcal{C}$ group and for any finite simple group S. The next three results are intended to reprove this result but without the restriction on the number of primes involved in $\mathcal{C}$.

Lemma 8.6.1 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F(X)$ be a free pro-$\mathcal{C}$ group on a set X converging to 1 with $|X| \geq 2$. Let Φ be the abstract subgroup of F generated by X. Assume that H is a closed normal subgroup of F of infinite index such that $H \cap \Phi \neq 1$. Then there exists an open normal subgroup U of F containing H and a basis X' of U converging to 1 such that $H \cap X' \neq \emptyset$.*

Proof. By Corollary 3.3.14, Φ is a free abstract group on the basis X. Let $\{U_i \mid i \in I\}$ be the collection of all open normal subgroups of F containing H; then $H = \bigcap_{i \in I} U_i$. For $i \in I$, denote by $\mathcal{X}_i$ the set of all bases Z of the abstract free group $U_i \cap \Phi$ such that Z is a basis converging to 1 of U_i. The set $\mathcal{X}_i$ is not empty by Theorem 3.6.2. Let $1 \neq w \in H \cap \Phi$. Then $w \in \Phi \cap U_i$ for each $i \in I$. For $Y \in \mathcal{X}_i$, let $\ell(Y)$ denote the word length of w with respect to the abstract basis Y of $\Phi \cap U_i$ and set

$$\ell = \min\{\ell(Y) \mid Y \in \mathcal{X}_i, i \in I\}.$$

Choose $j \in I$ and $X_j \in \mathcal{X}_j$ such that $\ell = \ell(X_j)$. Say $w = x_1^{\varepsilon_1} \cdots x_\ell^{\varepsilon_\ell}$ ($\varepsilon_r = \pm 1, x_r \in X_j, r = 1, \ldots, \ell$). We shall show that $x_1 \in H$. To see this, assume to the contrary that $x_1 \notin H$; then there exists some $k \in I$ such that $x_1 \notin U_k$ and U_k is a proper subgroup of U_j. Choose a Schreier transversal T of U_k in U_j containing $x_1^{\varepsilon_1}$ (the existence of such T is easily seen using, for example, Proposition I.14 in Serre [1980]). Then, using the notation of Theorem 3.6.2, the set

$$X(k) = \{s_{t,x} = tx\widetilde{tx}^{-1} \mid t \in T, x \in X_j, s_{t,x} \neq 1\}$$

is in $\mathcal{X}_k$. Moreover, if we put $t_1 = 1$ and $t_s = \widetilde{x_1^{\varepsilon_1} \cdots x_{s-1}^{\varepsilon_{s-1}}}$ ($s = 2, \ldots, \ell + 1$),

$$w = (t_1 x_1^{\varepsilon_1} t_2^{-1})(t_2 x_2^{\varepsilon_2} t_3^{-1}) \cdots (t_\ell x_\ell^{\varepsilon_\ell} t_{\ell+1}^{-1}), \tag{4}$$

since $t_{\ell+1} = 1$. Note that $t_1 x_1^{\varepsilon_1} t_2^{-1} = 1$, and that

$$t_s x_s^{\varepsilon_s} t_{s+1}^{-1} = \begin{cases} t_s x_s \widetilde{t_s x_s}^{-1}, & \text{if } \varepsilon_s = 1; \\ (t_{s+1} x_s \widetilde{t_{s+1} x_s}^{-1})^{-1}, & \text{if } \varepsilon_s = -1. \end{cases}$$

It follows that (4) is a word for w in terms of the basis $X(k)$, and so $\ell(X(k)) < \ell$, contradicting the choice of ℓ. Therefore $x_1 \in H$. If we set $U = U_j$ and $X' = X_j$, we deduce that X' is a basis of U' converging to 1 and $H \cap X' \neq \emptyset$, as desired. □

Proposition 8.6.2 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let F be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}$, with $\mathfrak{m} \geq 2$. Assume that N is a closed normal subgroup of F of infinite index. Let X be a basis of F converging to 1 and let Φ be the subgroup of F generated by X as an abstract group. If $\Phi \cap N \neq 1$, then $r_S(N) = \max\{\mathfrak{m}, \aleph_0\}$ for each simple group $S \in \mathcal{C}$.*

Proof. By Lemma 8.2.5, $r_S(N) \le \max\{\mathfrak{m}, \aleph_0\}$. We shall show that $r_S(N) \ge \max\{\mathfrak{m}, \aleph_0\}$. According to Lemma 8.6.1, we may assume that $X \cap N \neq \emptyset$.

Case 1. $\mathfrak{m} = |X|$ is finite.

Fix a natural number t. Set $G = F/N$ and $d = d(G)$. From $X \cap N \neq \emptyset$, we deduce that $d < \mathfrak{m}$. Since G is infinite, there exists an open subgroup U of G of index j sufficiently large so that $(\mathfrak{m} - d)j \ge t + d(S)$. Let V be the preimage of U in F. Then, according to Theorem 3.6.2, V is a free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(n)$ of rank $n = (\mathfrak{m} - 1)j + 1$. Moreover, $d(U) \le k = (d-1)j + 1$, by Corollary 3.6.3. Since $U \cong V/N$, we deduce from Lemma 8.2.5(d) and (b) that

$$r_S(N) \ge r_S(V) - r_S(U) \ge r_S(F_{\mathcal{C}}(n)) - r_S(F_{\mathcal{C}}(k)).$$

Now, if $r_S(F_{\mathcal{C}}(k)) = 0$, we have

$$r_S(N) \ge r_S(F_{\mathcal{C}}(n)) \ge r_S(F_{\mathcal{C}}((\mathfrak{m}-1)j)) \ge r_S(F_{\mathcal{C}}(t + d(S))) \ge t$$

by Lemma 8.2.7. On the other hand, if $r_S(F_{\mathcal{C}}(k)) \neq 0$, we can use Lemma 8.2.7 again to obtain

$$r_S(N) \ge r_S(F_{\mathcal{C}}(n)) - r_S(F_{\mathcal{C}}(k)) \ge n - k = (\mathfrak{m} - d)j \ge t.$$

Since t is arbitrary, we infer that

$$r_S(N) \ge \aleph_0.$$

Case 2. $\mathfrak{m} = |X| = \aleph_0$.

Fix $x \in X \cap N$. Let t be a natural number bigger than $d(S)$ and let Y be a finite subset of X of cardinality t such that $x \in Y$. Consider the epimorphism

$$\varphi : F_{\mathcal{C}}(X) \longrightarrow F_{\mathcal{C}}(Y)$$

that sends Y to Y identically and $X - Y$ to 1. Let $K = \varphi(N)$. Then $x \in K \cap Y$ and $K \triangleleft_c F_{\mathcal{C}}(Y)$. If $[F_{\mathcal{C}}(Y) : K] = \aleph_0$, we get that

$$r_S(N) \ge r_S(K) = \aleph_0,$$

by Case 1. If $[F_{\mathcal{C}}(Y) : K] = j < \aleph_0$, then by Theorem 3.6.2, K is free of rank $j(t-1) + 1$. So, by Lemma 8.2.7,

$$r_S(N) \ge r_S(K) = r_S(F_{\mathcal{C}}(j(t-1)+1)) \ge t - d(S) + r_S(F_{\mathcal{C}}(d(S))).$$

Since t is arbitrarily large, it follows that

$$r_S(N) \ge \aleph_0.$$

Case 3. $\mathfrak{m} = |X| > \aleph_0$.

Again, fix $x \in X \cap N$. We consider two subcases. First assume that S is nonabelian. Let I denote an indexing set with the same cardinality as X, and consider the direct product

$$E = \prod_{i \in I} S_i$$

where $S_i \cong S$ for all $i \in I$. Observe that $\bigcup_{i \in I} S_i$ is a set of generators of E converging to 1. Choose $\mathbf{s} = (s_i) \in E$ to be such that $s_i \neq 1$ for every $i \in I$. Then there exists an epimorphism

$$\varphi : F \longrightarrow E = \prod_{i \in I} S_i$$

such that $\varphi(x) = \mathbf{s}$. Since S is simple and nonabelian and since $x \in N$, we infer from Lemma 8.2.4 that $\varphi(N) = E$. Thus, $r_S(N) \geq |I| = |X| = \mathfrak{m}$.

Next, assume that $S \cong \mathbf{Z}/p\mathbf{Z}$, where p is a prime number. Let R denote the intersection of the open normal subgroups of F whose index is a finite power of p. Then $\tilde{F} = F/R$ is the free pro-p group on the set X (see Proposition 3.4.2). Let $\tilde{N} = NR/R$. Then $\tilde{N}$ is a closed normal subgroup of $\tilde{F}$. If $[\tilde{F} : \tilde{N}] < \infty$, then $\operatorname{rank}(\tilde{N}) = |X|$ by Theorem 3.6.2; hence $r_p(\tilde{N}) = |X|$ by Proposition 8.2.6. Therefore, $r_p(N) \geq |X|$. If $[\tilde{F} : \tilde{N}]$ is not finite, the result follows from Proposition 8.6.3 below. □

Proposition 8.6.3 *Let p be a prime number and let $F = F_p(X)$ be a free pro-p group on a set X converging to* 1, *where $|X| \geq 2$. Assume that N is a closed nontrivial normal subgroup of F of infinite index. Then,*

$$\operatorname{rank}(N) = \max\{|X|, \aleph_0\}.$$

Proof. Note that in this case $M_p(F) = M(F) = \Phi(F)$, the Frattini subgroup of F. By Proposition 2.1.4, $N = \bigcap U$, where U runs through the open normal subgroups of F containing N. It follows that (see Proposition 2.8.9)

$$\Phi(N) = \varprojlim \Phi(U) = \bigcap \Phi(U).$$

Since N is nontrivial, we have $\Phi(N) \neq N$. So, there exists some U such that $N \leq U \triangleleft_o F$ and $N \not\leq \Phi(U)$, that is, such that $N - (N \cap \Phi(U)) \neq \emptyset$. Choose $y \in N - (N \cap \Phi(U))$. By Corollary 7.6.10, there exists a basis Y converging to 1 of the free pro-p group U with $y \in Y$ (note that U is free pro-p by Theorem 3.6.2). Hence, replacing F by U if necessary, we may assume that $X \cap N \neq \emptyset$.

Then the hypotheses of cases 1 and 2 in the proof of Proposition 8.6.2 are valid under our present assumptions, and therefore our result holds if $|X| \leq \aleph_0$.

Suppose next that $|X| > \aleph_0$. We know that N is a free pro-p group (see Corollary 7.7.5). If $\operatorname{rank}(N) = |X|$, then $r_p(N) = \operatorname{rank}(N) = |X|$ by Proposition 8.2.6; hence, in this case, the result follows.

The other alternative is that $\text{rank}(N) < |X|$; but we shall show presently that this in fact is not possible. Indeed, assume that $\text{rank}(N) < |X|$. Then, by Lemma 8.3.8(b), there exist closed subgroups L and R of F such that $N, R \le L \triangleleft F$, $L = N \times R$ and $w_0(F/L) \le w_0(N)$. Remark that $w_0(N) < |X| = w_0(F)$, because either N has finite rank and then $w_0(N) = \aleph_0$, or $w_0(N) = \text{rank}(N)$. It follows that $w_0(F/L) < |X|$; hence, $w_0(L) = |X|$, and so $w_0(R) = |X|$. Choose elements x and y such that $1 \ne x \in N$ and $1 \ne y \in R$. By Corollary 7.7.5, $\overline{\langle x, y\rangle}$ is a free pro-p group. Since $xy = yx$, this group is abelian, and hence $\overline{\langle x, y\rangle} = \overline{\langle z\rangle}$, for some element z. On the other hand, it is plain that

$$\overline{\langle z\rangle} = \overline{\langle x, y\rangle} = \overline{\langle x\rangle} \times \overline{\langle y\rangle}.$$

Say $x = z^\alpha$ and $y = z^\beta$. Then $\overline{\langle x\rangle} \cap \overline{\langle y\rangle} \ge \overline{\langle z^{\alpha\beta}\rangle} \ne 1$. This contradiction implies that, in fact, the case $\text{rank}(N) < |X|$ never occurs. □

Corollary 8.6.4 *Let $\mathcal{C}$ be an NE-formation of finite groups and let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \ge 2$. Let N be a closed normal subgroup of F. Assume that either $\mathfrak{m}$ or the index of N in F is infinite. Then for any given prime number p, either $r_p(N) = 0$ or $r_p(N) = \mathfrak{m}^*$, where $\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$.*

Proof. Consider a prime number p for which $r_p(N) \ne 0$. Then there exists some $K \triangleleft_o N$ with $N/K \cong C_p$. We must show that $r_p(N) = \mathfrak{m}^*$, and for this it suffices to check that $r_p(N) \ge \mathfrak{m}^*$. By Lemma 8.3.8(b) there exists an open normal subgroup L of F containing N such that $K \triangleleft L$ and $L/K = N/K \times N'/K$, where N' is a certain closed normal subgroup of L containing K; furthermore, if the rank of F is finite, L can be chosen so that its rank is arbitrarily large. According to Theorem 3.6.2, L is free pro-$\mathcal{C}$ and $\max\{\text{rank}(L), \aleph_0\} = \max\{\mathfrak{m}, \aleph_0\}$. So, we may assume that $F = L$, and if $\text{rank}(F)$ is finite, we may suppose it is as large as we wish. It follows that $K = N \cap N'$ and $F/N' \cong N/K \cong C_p$. Recall that if $R = R_p(F)$ is the intersection of all closed normal subgroups T of F where F/T is a pro-p group, then F/R is the free pro-p group of rank $\mathfrak{m}$ (see Proposition 3.4.2). By Lemma 8.2.5, $r_p(N) \ge r_p(NR/R)$. Note that NR/R is nontrivial, for if $NR = R$, then $N \le R \le N'$ and so $NN' = N'$; however we know that $NN' = F \ne N'$. If the index of NR/R in F/R is infinite, then $r_p(N) \ge r_p(NR/R) = \mathfrak{m}^*$ by Proposition 8.6.3. Suppose now that $[F/R : NR/R] < \infty$. Then $r_p(NR/R) \ge \mathfrak{m}$ by Theorem 3.6.2 and Proposition 8.2.6. If $\mathfrak{m}$ is infinite, we clearly have $r_p(N) \ge r_p(NR/R) = \mathfrak{m} = \mathfrak{m}^*$. On the other hand, if $\mathfrak{m}$ is finite, we may assume that $r_p(NR/R)$ is as large as we wish; thus $r_p(N) \ge \aleph_0 = \mathfrak{m}^*$. Therefore, if $\mathfrak{m}$ is finite, then $r_p(N) = \aleph_0$. □

Theorem 8.6.5 *Let $\mathcal{C}$ be an NE-formation of finite groups. Assume that N is a closed normal subgroup of a free pro-$\mathcal{C}$ group $F = F_{\mathcal{C}}(\mathfrak{m})$ of rank $\mathfrak{m} \ge 2$. Then $d(N)$ is finite if and only if $\mathfrak{m}$ is finite and N has finite index in F.*

Proof. If $\mathcal{C}$ involves at least two primes, this follows from Corollary 8.5.12. If F is a pro-p group, then the result follows from Proposition 8.6.3 and Theorem 3.6.2. □

For varieties of finite groups we have the following result.

Theorem 8.6.6 *Let $\mathcal{C}$ be an extension closed variety of finite groups and let L be a finitely generated subgroup of a free pro-$\mathcal{C}$ group $F = F(\mathfrak{m})$ of rank $\mathfrak{m} \geq 2$. Suppose L contains a nontrivial normal subgroup N of F. Then $\mathfrak{m}$ is finite and L is open in F.*

Proof. If $\mathcal{C}$ involves at least two different primes, the result is a special case of Theorem 8.5.16. If F a free pro-p group, for completeness we indicate an easy proof based on Theorem 9.1.19 proved later on and on a result not contained in this book. According to Theorem 9.1.19, there exists an open subgroup U of F containing L such that $U = L \amalg L_1$ (the free pro-p product; see Section 9.1 for this concept). Since N is normal in F and nontrivial, $L \cap L^x \geq N \neq 1$, for every $x \in L_1$. This implies that $L_1 = 1$ (cf. Herfort and Ribes [1985], Theorem B′), i.e., $L = U$ is open. Since L is finitely generated, this means that $\mathfrak{m}$ is finite. □

Theorem 8.6.7 *Let $\mathcal{C}$ be an NE-formation of finite groups and let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of infinite rank $\mathfrak{m}$. Assume that N_1 and N_2 are closed normal subgroups of F with the same S-rank functions, i.e., $r_S(N_1) = r_S(N_2)$ for all $S \in \Sigma$. Then $N_1 \cong N_2$.*

Proof. If F is a free pro-p group, then N_1 and N_2 are free pro-p groups of rank $\mathfrak{m}$. Therefore $N_1 \cong N_2$. Assume next that $\mathcal{C}$ involves at least two different primes. Then by Theorems 3.6.2 and 8.5.4, the groups N_1 and N_2 are homogeneous and $w_0(N_1) = w_0(N_2)$. Then the result follows from Theorem 8.5.2. □

Theorem 8.6.8 *Let $\mathcal{C}$ be an NE-formation of finite groups and let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. A nontrivial closed normal subgroup N of infinite index in F is free pro-$\mathcal{C}$ if and only if $r_S(N) = \mathfrak{m}^*$ for every finite simple group $S \in \mathcal{C}$, where $\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$.*

Proof. If $\mathcal{C}$ involves at least two different primes, this follows from Theorem 8.5.13 and Theorem 3.6.2. If F is a free pro-p group, every closed subgroup N of F is free pro-p by Corollary 7.7.5; moreover if N is of infinite index in F, then $r_p(N) = \mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$ by Proposition 8.6.3. □

Example 8.6.9 Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free profinite group of rank $\mathfrak{m} \geq 2$. Let $\mathcal{S}$ be the class of all finite solvable groups. Let $R_{\mathcal{S}}(F)$ be as defined in Section 3.4, so that $F/R_{\mathcal{S}}(F)$ is the maximal prosolvable quotient of F. Then $R_{\mathcal{S}}(F)$ has no nontrivial prosolvable quotients (see Lemma 3.4.1). Hence, in particular, $R_{\mathcal{S}}(F)$ is not a free profinite group.

Similarly, for every prime number p, the normal subgroup $R_p(F)$ of F is not a free profinite group. Observe that if p and q are different primes, then, using Theorem 8.6.7, one sees that $R_p(F)$ and $R_q(F)$ are not isomorphic. Similarly, $R_p(F) \ncong R_{\mathcal{S}}(F)$.

Definition 8.6.10 *Let $\mathfrak{m}$ be an infinite cardinal. Denote by $\mathcal{X}_{\mathcal{C}}(\mathfrak{m})$ the collection of all functions $f = f_{\mathcal{C}}$ that assign to each finite simple group S a cardinal number $f(S)$ satisfying the following conditions*:

(a) $0 \leq f(S) \leq \mathfrak{m}$, *for all* $S \in \Sigma$;
(b) *If* $S \notin \Sigma_{\mathcal{C}}$, *then* $f(S) = 0$; *and*
(c) *For a prime number* p, $f(C_p)$ *is either* 0 *or* $\mathfrak{m}$.

The next two theorems indicate the importance of such functions f. They show that $\mathcal{X}_{\mathcal{C}}(\mathfrak{m})$ is exactly the collection of all S-rank functions of normal subgroups of a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}$.

Theorem 8.6.11 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$ and N a closed normal subgroup of F. Assume that either $\mathfrak{m}$ or the index of N in F is infinite. Then the S-rank function $r_*(N)$ of N belongs to $\mathcal{X}_{\mathcal{C}}(\mathfrak{m}^*)$, where $\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$.*

Proof. If $N = 1$, the result is obvious. Assume $N \neq 1$. By Lemma 8.2.5, $r_S(N) \leq w_0(N) \leq w_0(F) = \mathfrak{m}^*$ for $S \in \Sigma$, and obviously $r_S(N) = 0$ for $S \notin \Sigma_{\mathcal{C}}$. The function $r_*(N)$ satisfies condition (c) by Corollary 8.6.4. □

Theorem 8.6.12 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $\mathfrak{m}$ be an infinite cardinal and let $f \in \mathcal{X}_{\mathcal{C}}(\mathfrak{m})$. Then $F = F_{\mathcal{C}}(\mathfrak{m})$ contains a closed normal subgroup N with rank function $r_*(N)$ such that $f(S) = r_S(N)$ for every $S \in \Sigma_{\mathcal{C}}$.*

Proof. Recall that $\Sigma_{\mathcal{C}}$ is the collection of all simple groups in $\mathcal{C}$.

Step 1. Construction of N.

For each $S \in \Sigma_{\mathcal{C}}$, choose K_S to be a closed normal subgroup of F such that

$$M_S(F) \leq K_S \leq F$$

and

$$r_S(K_S/M_S(F)) = f(S).$$

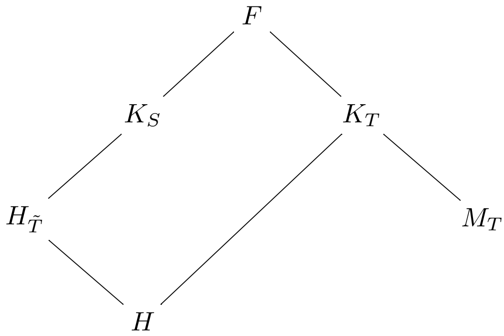
Put

$$H = \bigcap_{S \in \Sigma_{\mathcal{C}}} K_S.$$

We claim that $HM_T(F) = K_T$ for each $T \in \Sigma_{\mathcal{C}}$. To see this, first set

$$H_{\tilde{T}} = \bigcap_{S \neq T} K_S.$$

Remark that $F/H_{\tilde{T}}$ does not admit T as a quotient, since $F/H_{\tilde{T}}$ is a quotient of $F/(\bigcap_{S\neq T} M_S(F))$.



We deduce that $F/H_{\tilde{T}}K_T = 1$, since $F/H_{\tilde{T}}K_T$ is a quotient of both $F/H_{\tilde{T}}$ and F/K_T. So $F = H_{\tilde{T}}K_T$; therefore $K_T/H \cong F/H_{\tilde{T}}$ does not admit T as a quotient. Now, since $K_T/HM_T(F)$ is a product of copies of T as well as a quotient of K_T/H, we have $HM_T(F) = K_T$, proving the claim.

Consider now the set $\mathcal{L}$ of all closed normal subgroups L of F such that $LM_T(F) = K_T$ for each $T \in \Sigma_{\mathcal{C}}$. Since $H \in \mathcal{L}$, $\mathcal{L} \neq \emptyset$. Define a partial ordering on $\mathcal{L}$ by reverse inclusion, i.e., $L_1 \prec L_2$ if and only if $L_1 \geq L_2$. Then $(\mathcal{L}, \prec)$ is an inductive poset. Indeed, let $\{L_i \mid i \in I\}$ be a totally ordered subset of $\mathcal{L}$, and set $L = \bigcap_{i\in I} L_i$; then $LM_T(F) = K_T$ for each $T \in \Sigma_{\mathcal{C}}$ (to see this, let $k \in K_T$; then the nonempty closed subsets $B_i = L_i \cap kM_T(F)$ $(i \in I)$ have the finite intersection property; hence, by the compactness of F, $\bigcap_{i\in I} B_i = L \cap kM_T(F) \neq \emptyset$, i.e., $k \in LM_T(F)$). By Zorn's Lemma there exists a maximal N in the poset $(\mathcal{L}, \prec)$. Therefore, N is a minimal closed normal subgroup of F with respect to the property

$$NM_T(F) = K_T \quad \text{for all } T \in \Sigma_{\mathcal{C}}.$$

Step 2. We shall show that for this N, $r_S(N) = f(S)$ for every finite simple group S.

Clearly, $r_S(N) = 0$ if $S \notin \Sigma_{\mathcal{C}}$, and $r_S(N) \leq \mathfrak{m}$ for each $S \in \Sigma_{\mathcal{C}}$ (see Lemma 8.2.5). Assume $S \in \Sigma_{\mathcal{C}}$ and $f(S) = \mathfrak{m}$. Since $NM_S(F) = K_S$, there is an epimorphism from N onto $K_S/M_S(F)$; so $r_S(N) \geq r_S(K_S/M_S(F)) = \mathfrak{m}$; thus $r_S(N) = f(S)$.

Next suppose that $S \in \Sigma_{\mathcal{C}}$ and $f(S) = 0$. We claim that $M_S(N)$ is in the set $\mathcal{L}$ defined in Step 1 above. Since $M_S(F) = K_S$, one has $N \leq M_S(F)$, and hence $M_S(N)M_S(F) = K_S$. For $T \in \Sigma_{\mathcal{C}}$, $T \neq S$, observe that the image of the natural epimorphism

$$N/M_S(N) \longrightarrow NM_T(F)/M_S(N)M_T(F) = K_T/M_S(N)M_T(F)$$

must be trivial, since $N/M_S(N)$ is a direct product of copies of S, and $K_T/M_S(N)M_T(F)$ a direct product of copies of T. Therefore

$$M_S(N)M_T(F) = K_T,$$

proving our claim. From the minimality of N, we infer that $M_S(N) = N$. Thus $r_S(N) = 0$, as needed.

Finally, let $S \in \Sigma_{\mathcal{C}}$ with $0 \neq f(S) \neq \mathfrak{m}$. In particular, S is not abelian. To verify that $r_S(N) = f(S)$, it suffices to show that $N \cap M_S(F) = M_S(N)$. Indeed, if that is the case,

$$N/M_S(N) \cong NM_S(F)/M_S(F) = K_S/M_S(F),$$

and, by assumption, $r_S(K_S/M_S(F)) = f(S)$.

Suppose $N \cap M_S(F) \neq M_S(N)$. Then there exists $U \triangleleft_o N$ with $N/U \cong S$ such that for every $V \triangleleft_o F$ with $F/V \cong S$, one has $V \cap N \neq U$. For any such V we have either $N \leq V$, and then $NV = V = UV$, or $N \not\leq V$, and then $NV = F = UV$. Therefore, for any $x \in F$, one has

$$x^{-1}UxV = x^{-1}UVx = x^{-1}NVx = NV.$$

Set

$$R = \bigcap_{x \in F} x^{-1}Ux.$$

Now, if $N \leq V$, then $RV = V$. On the other hand, if $N \not\leq V$, $RV = F$ by Lemma 8.2.1, since S is a nonabelian simple group, and, as pointed out above, $x^{-1}UxV = F$ for all $x \in F$. Hence

$$NV = RV \quad \text{for all } V \triangleleft_o F \text{ with } F/V \cong S.$$

Therefore, taking intersections over these V,

$$\bigcap_V RV = \bigcap_V NV.$$

Now,

$$\bigcap_V RV = \bigcap_{V \geq R} RV = \bigcap_{V \geq RM_S(F)} V = RM_S(F),$$

since $RM_S(F)$ is normal in F (see Lemma 8.2.4 for the last equality). Similarly,

$$\bigcap_V NV = \bigcap_{V \geq N} NV = \bigcap_{V \geq NM_S(F)} V = NM_S(F) = K_S.$$

Thus $RM_S(F) = K_S$. Further, we shall show that $R \in \mathcal{L}$. To see this it remains to show that if $S \neq T \in \Sigma_{\mathcal{C}}$, then $RM_T(F) = K_T$. First observe that N/R is a direct product of copies of S (see Lemma 8.2.2), and hence so is its homomorphic image $NM_T(F)/RM_T(F) = K_T/RM_T(F)$. But this last group is a direct product of copies of T. Thus $K_T = RM_T(F)$. So $R \in \mathcal{L}$. By the minimality of N, we get that $R = N$, a contradiction. Hence U does not exist. Therefore $N \cap M_S(F) = M_S(N)$, as desired. □

Theorem 8.6.13 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of finite rank $\mathfrak{m} \geq 2$ and let N be a closed normal subgroup of F of infinite index. Then N is isomorphic to a normal subgroup of $F_{\mathcal{C}}(\aleph_0)$ (in fact to any closed normal subgroup of $F_{\mathcal{C}}(\aleph_0)$ whose rank function is $r_*(N)$).*

Proof. If $\mathcal{C}$ involves only one prime p, then the result is clear since then N is a free pro-p group of countably infinite rank (see Proposition 8.6.3). Assume that $\mathcal{C}$ involves at least two different primes. Then N is homogeneous by Theorem 8.5.4. By Theorem 8.6.11, $r_*(N) \in \mathcal{X}_{\mathcal{C}}(\aleph_0)$; and according to Theorem 8.6.12, there exists a closed normal subgroup N_1 of $F_{\mathcal{C}}(\aleph_0)$ such that $r_*(N_1) = r_*(N)$. If N_1 has finite index in $F_{\mathcal{C}}(\aleph_0)$, then it is isomorphic to $F_{\mathcal{C}}(\aleph_0)$ (see Theorem 3.6.2); therefore, N_1 is homogeneous. If, on the other hand, the index of N_1 is infinite, then N_1 is homogeneous by Theorem 8.5.4. Thus, by Theorem 8.5.2, $N \cong N_1$. The last assertion of the theorem follows from Theorem 8.6.7. □

Exercise 8.6.14 Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of finite rank $\mathfrak{m} \geq 2$ and N a closed normal subgroup of F of infinite index. Then N is isomorphic to a normal subgroup of $F_{\mathcal{C}}(\aleph_0)$.

Exercise 8.6.15 Let π be a nonempty set of prime numbers and let $\mathcal{C}$ be the class of all finite solvable groups whose orders involve only primes in π. Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be the free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$ and let N be a nontrivial closed normal subgroup of F of infinite index. Let $\mathcal{C}'$ be the class of all finite solvable groups whose orders involve only those primes $p \in \pi$ such that C_p is not a (continuous) quotient of N.

(a) $\mathcal{C}$ and $\mathcal{C}'$ are extension closed varieties of finite solvable groups.
(b) The isomorphism class of N is determined by the primes involved in $\mathcal{C}'$ in the following sense. Let $\mathfrak{m}^* = \{\mathfrak{m}, \aleph_0\}$ and let $R = R_{\mathcal{C}'}(F_{\mathcal{C}}(\mathfrak{m}^*))$ be the intersection of all closed normal subgroups M of the free pro-$\mathcal{C}$ group $F_{\mathcal{C}}(\mathfrak{m}^*)$ of rank $\mathfrak{m}^*$ such that $F_{\mathcal{C}}(\mathfrak{m}^*)/M$ is pro- $\mathcal{C}'$. Then

$$N \cong R.$$

8.7 Proper Open Subgroups of Normal Subgroups

In Example 8.6.9 we saw explicit instances of closed normal subgroups of a free pro-$\mathcal{C}$ group which are not free pro-$\mathcal{C}$. The main result of this section is that any proper open normal subgroup of closed normal subgroups of a free pro-$\mathcal{C}$ group are free pro-$\mathcal{C}$. This follows immediately from the work above and it is stated in Theorem 8.7.1. A more general result holds if $\mathcal{C}$ is an extension closed variety of finite groups. In this case, any proper open subgroup of a closed normal subgroups of a free pro-$\mathcal{C}$ group is free pro-$\mathcal{C}$. This result requires some additional preparation and it is proved in Theorem 8.7.9.

Theorem 8.7.1 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let F be a free pro - $\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$ and N a closed normal subgroup of F. Then, every proper open normal subgroup K of N is a free pro - $\mathcal{C}$ group.*

Proof. If F is a free pro-p group, then the result is clear by Corollary 7.7.5. Assume that $\mathcal{C}$ involves at least two different primes. By Theorem 3.6.2 we may assume that N has infinite index in F. Next observe that if p is a prime number and N/K is a p-group, then $r_p(N) = \mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$ by Corollary 8.6.4. Therefore, by Theorem 8.5.14, $r_S(K) = \mathfrak{m}^*$ for every finite simple group S in $\mathcal{C}$. Thus K is free pro - $\mathcal{C}$ by Theorem 8.5.13. □

Proposition 8.7.2 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F(\mathfrak{m})$ be a free pro - $\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Then, every closed abelian normal subgroup of F is trivial.*

Proof. Let $N \triangleleft_c F$. If $[F : N] < \infty$, then N is free pro - $\mathcal{C}$ of rank at least 2 according to Theorem 3.6.2; hence N is not abelian. If $[F : N]$ is infinite, then it contains a proper normal subgroup T, which is free pro - $\mathcal{C}$ by Theorem 8.7.1. Using Theorem 8.6.5 one deduces that the rank of T is infinite, and thus T is not abelian. □

Corollary 8.7.3 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F(\mathfrak{m})$ be a free pro - $\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Then, the center of F is trivial.*

Proposition 8.7.4 *Let $\mathcal{C}$ be an NE-formation of finite groups involving at least two different prime numbers. Let $F = F(\mathfrak{m})$ be a free pro - $\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Then, every closed pronilpotent normal subgroup of F is trivial.*

Proof. Let p, q be distinct primes such that $C_p, C_q \in \mathcal{C}$. Consider the wreath product $G = C_p \wr C_q$. Then $G \in \mathcal{C}$, $d(G) = 2$ and G is not nilpotent. Let N be a nontrivial closed normal subgroup of F. If $[F : N] < \infty$, then N is free pro - $\mathcal{C}$ of rank at least 2 according to Theorem 3.6.2; hence there is a continuous epimorphism $N \longrightarrow G$, and so N is not pronilpotent. Assume that $[F : N] = \infty$. Let K be a proper open normal subgroup of N. By Theorems 8.7.1 and 8.5.16, K is free pro - $\mathcal{C}$ of infinite rank. Hence G is a homomorphic image of K. Therefore K is not pronilpotent, and so neither is N. □

Since the Frattini subgroup of a profinite group is pronilpotent (see Corollary 2.8.4), we deduce

Corollary 8.7.5 *Let $\mathcal{C}$ be an NE-formation of finite groups involving at least two different prime numbers. Let $F = F(\mathfrak{m})$ be a free pro - $\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Then, the Frattini subgroup of F is trivial.*

Exercise 8.7.6

(a) Prove that results 8.6.2–8.6.8, 8.6.11 and 8.7.1–8.7.4 remain valid for subnormal subgroups N.

(b) Show that Theorem 8.7.1 is not necessarily valid if one only assumes that N is an accessible subgroup, even if $\mathcal{C}$ is an NE-formation of finite groups involving at least two different prime numbers.

Proposition 8.7.7 *Let $\mathcal{C}$ be an NE-formation of finite groups. A free pro-$\mathcal{C}$ group $F = F(\mathfrak{m})$ of rank $\mathfrak{m} \geq 2$ cannot be written as a nontrivial direct product.*

Proof. Suppose $F = A \times B$, where $A \neq 1 \neq B$. Choose open normal proper subgroups A_1 and B_1 of A and B respectively. By Theorem 8.7.1, A_1 and B_1 are free pro-$\mathcal{C}$. Choose a prime p such that $C_p \in \mathcal{C}$. Then F contains a closed subgroup isomorphic to $\mathbf{Z}_p \times \mathbf{Z}_p$. Hence (see Theorem 7.3.1 and Exercise 7.4.3) the cohomological dimension of F would be at least 2, a contradiction. □

We can now generalize Corollary 8.7.3.

Proposition 8.7.8 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let F be a pro-$\mathcal{C}$ group of rank at least two, and let $N \triangleleft_c F$. Then the centralizer $\mathrm{C}_F(N)$ of N in F is trivial.*

Proof. Put $C = \mathrm{C}_F(N)$. Then $C \cap N$ is an abelian normal subgroup of F, and hence $C \cap N = 1$ by Corollary 8.7.3. Therefore, $CN = C \times N$. If $C \neq 1$, let C_1 be a proper open normal subgroup of C. Then by Theorem 8.7.1, the group $C_1 \times N$ is a free pro-$\mathcal{C}$ group. This contradicts the conclusion of Proposition 8.7.7. Thus $C = 1$. □

Next we state a sharper version of Theorem 8.7.1 when the class $\mathcal{C}$ is in addition a variety.

Theorem 8.7.9 *Let $\mathcal{C}$ be an extension closed variety of finite groups and let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Let N be a closed normal subgroup of F and R a proper open subgroup of N. Then R is a free pro-$\mathcal{C}$ group. If either $[F : N] = \infty$ or $\mathfrak{m} = \infty$, then $\mathrm{rank}(R) = \mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$; while, if $[F : N] < \infty$ and $\mathfrak{m} < \infty$, then $\mathrm{rank}(R) = [F : R](\mathfrak{m} - 1) + 1$.*

The proof of this theorem consists of first reducing the problem to the situation when R is a normal subgroup of infinite index of a free pro-$\mathcal{C}$ group; then one uses Theorem 8.6.8. The key step is contained in the following lemma; it will allow us to compute the rank function of R.

Lemma 8.7.10 *Let $\mathcal{C}$ be an extension closed variety of finite groups, and let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of infinite rank $\mathfrak{m}$. Let E be a proper open subgroup of F. Let S be a finite simple group in $\mathcal{C}$. Then there exists a closed normal subgroup H of E such that $H(E \cap M_S(F)) = E$ and $E/H \cong \prod_{\mathfrak{m}} S$.*

Proof. We shall use the fact that S can be generated by two elements; but the proof can be easily modified if one does not want to use this fact.

Let I denote a set of cardinality $\mathfrak{m}$. Let $X = Y \cup \{x_i, x_i' \mid i \in I\}$ be a basis of F converging to 1 such that $X \cap E = \{x_i, x_i' \mid i \in I\}$. Note that Y is finite. For each $i \in I$ define a continuous epimorphism

$$\varphi_i : F \longrightarrow S$$

such that $\varphi_i(y) = 1$ for $y \in Y$ and

$$\overline{\langle \varphi_i(x_j), \varphi_i(x_j') \rangle} = \begin{cases} S & \text{if } j = i; \\ 1 & \text{if } j \neq i. \end{cases}$$

If S is abelian, we shall assume in addition that $\varphi_i(x_j) = \varphi_i(x_j')$ for all $j \in I$. Clearly, $E \cap M_S(F)$ is a closed normal subgroup of $E \cap (\bigcap_{i\in I} \operatorname{Ker}(\varphi_i))$. Define $\psi_i : E \longrightarrow S$ to be the restriction of φ_i to E. Set

$$M = E \cap \left(\bigcap_{i \in I} \operatorname{Ker}(\varphi_i) \right) = \bigcap_{i \in I} \operatorname{Ker}(\psi_i).$$

Hence it suffices to show the existence of a closed normal subgroup H of E such that $HM = E$ and $E/H \cong \prod_{\mathfrak{m}} S$.

By the construction in the proof of Theorem 3.6.2, E admits a basis $W = \{x_i, x_i' \mid i \in I\} \cup Z$ converging to 1, where Z has cardinality $\mathfrak{m}$. Furthermore, the elements of Z have the form $tx(\widetilde{tx})^{-1} (\neq 1)$, where t ranges through a certain right transversal T, containing 1, of E in F, and where $x \in X$.

For each $i \in I$, define

$$\sigma_i : E \longrightarrow S$$

to be a continuous epimorphism such that $\sigma_i(z) = 1$ for all $z \in Z$ and

$$\overline{\langle \sigma_i(x_j), \sigma_i(x_j') \rangle} = \begin{cases} S & \text{if } j = i; \\ 1 & \text{if } j \neq i. \end{cases}$$

If S is abelian, we shall assume in addition that $\sigma_i(x_j) = \sigma_i(x_j')$ for all $j \in I$. It follows from this definition that $\operatorname{Ker}(\sigma_i) \neq \operatorname{Ker}(\sigma_j)$ for all $i, j \in I$, $i \neq j$.

Next we claim that $\operatorname{Ker}(\sigma_i) \neq \operatorname{Ker}(\psi_j)$ for all $i, j \in I$. Assume to the contrary that $\operatorname{Ker}(\sigma_i) = \operatorname{Ker}(\psi_j)$. Choose $x \in \{x_i, x_i'\}$ and $1 \neq t \in T$ (such t exists since $[F : E] > 1$) so that $tx(\widetilde{tx})^{-1} \in Z$. Then $\sigma_i(tx(\widetilde{tx})^{-1}) = 1$, and therefore (note $\widetilde{tx} = t$, since $x \in E$)

$$1 = \psi_j(tx(\widetilde{tx})^{-1}) = \varphi_j(tx(\widetilde{tx})^{-1}) = \varphi_j(txt^{-1}) = \varphi_j(t)\varphi_j(x)\varphi_j(t)^{-1}.$$

Hence, $\varphi_j(x) = 1$, and so $\psi_j(x) = 1$. Thus $\sigma_i(x) = 1$; but, by definition of σ_i, $\sigma_i(x) \neq 1$, a contradiction. This proves the claim.

Define $H = \bigcap_{i\in I} \operatorname{Ker}(\sigma_i)$.

Case 1: S is nonabelian.

Then, by Lemma 8.2.3, the canonical homomorphism

$$E/H \longrightarrow \prod_{i\in I} E/\mathrm{Ker}(\sigma_i)$$

is an isomorphism. Therefore,

$$E/H \cong \prod_{\mathfrak{m}} S.$$

Finally, we have to show that $HM = E$. Suppose not. Then, by Lemma 8.2.4, there exists an open normal subgroup L of E such that $L = \mathrm{Ker}(\sigma_i) = \mathrm{Ker}(\psi_j)$, for some $i, j \in I$. This contradicts the claim above.

Case 2: $S \cong \mathbf{Z}/p\mathbf{Z}$ is cyclic of prime order p.

In this case, let $E/R_p(E)$ be the maximal pro-p quotient of E. Then $E/R_p(E)$ is free pro-p of rank $\mathfrak{m}$. Observe that E/H is the Frattini quotient of $E/R_p(E)$. Therefore, $w_0(E/H) = \mathfrak{m}$; so, $E/H \cong \prod_{\mathfrak{m}} \mathbf{Z}/p\mathbf{Z}$.

It remains to prove that $E = HM$. To show this, consider the $\mathbf{Z}/p\mathbf{Z}$-vector space $V = E/M_p(E)$, written additively. Let $\bar{H}$ and $\bar{M}$ denote the canonical images of H and M in V, respectively.

It suffices to prove that $\bar{H} + \bar{M} = V$. Denote by $\bar{\psi}_i : V \longrightarrow \mathbf{Z}/p\mathbf{Z}$ and $\bar{\sigma}_i : V \longrightarrow \mathbf{Z}/p\mathbf{Z}$ the maps induced on V by ψ_i and σ_i respectively ($i \in I$). Then, using the notation of Section 2.9, we have $\bar{M} = \mathrm{Ann}_V(\langle \bar{\psi}_i \mid i \in I\rangle)$ and $\tilde{H} = \mathrm{Ann}_V(\langle \bar{\sigma}_i \mid i \in I\rangle)$. Hence, according to Proposition 2.9.10,

$$\bar{H} + \bar{M} = \mathrm{Ann}_V(\langle \bar{\psi}_i \mid i \in I\rangle \cap \langle \bar{\sigma}_i \mid i \in I\rangle).$$

Therefore, it suffices to show that $\langle \bar{\psi}_i \mid i \in I\rangle \cap \langle \bar{\sigma}_i \mid i \in I\rangle = 0$. To see this, consider an element α in this intersection. Say

$$\alpha = \sum_{i\in I} a_i \bar{\psi}_i = \sum_{i\in I} b_i \bar{\sigma}_i,$$

where $a_i, b_i \in \mathbf{Z}/p\mathbf{Z}$, and all coefficients a_i, b_i are zero but for a finite number of cases. We must show that $\alpha = 0$. Consider the image $\bar{z}$ in V of an element $z = tx_i\widetilde{tx_i}^{-1} \in Z$ ($i \in I$, $1 \neq t \in T$). Then

$$\bar{\psi}_j(\bar{z}) = \psi_j(tx_i\widetilde{tx_i}^{-1}) = \psi_j(tx_it^{-1}) = \psi_j(t) + \psi_j(x_i) - \psi_j(t) = \varphi_j(x_i).$$

By definition of φ_i we have that $\varphi_j(x_i) = 0$ if and only if $j \neq i$. On the other hand, $\bar{\sigma}_j(\bar{z}) = 0$ for all $j \in I$. Therefore, $a_i = 0$ for all $i \in I$. Thus $\alpha = 0$. □

Proof of Theorem 8.7.9. If $[F : N] < \infty$, the result follows from Theorem 3.6.2. Suppose $[F : N]$ is infinite. By Theorem 8.6.13 we may assume that $\mathfrak{m}$ is an infinite cardinal. By Theorem 8.6.8, it suffices to prove that $r_S(R) = \mathfrak{m}$ for every finite simple group $S \in \mathcal{C}$. Choose an open subgroup E of F with $E \cap N = R$. Replacing F by EN if necessary, we may assume that $F = EN$. By Theorem 3.6.2, E is a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}$. Given any finite simple group $S \in \mathcal{C}$, it follows from Lemma 8.7.10 that there exists a closed normal subgroup H of E such that $E/H \cong \prod_{\mathfrak{m}} S$ and $H(E \cap M_S(F)) = E$. We claim that $HR = E$. Suppose not. Then there exists a closed normal subgroup K of E such that $E/K \cong S$ and $K \geq HR$ (this assertion is clear if $S = C_p$ for some prime p, for in this case E/H is an elementary abelian p-group; while, if S is nonabelian, the assertion follows from Lemma 8.2.4). Put $L = NK$. Then $L \triangleleft F$ and $F/L \cong S$. Therefore $K = L \cap E \geq M_S(F)$. Thus $K \geq HM_S(F)$, contradicting the fact that $E = HM_S(F)$. This proves the claim. Hence,

$$R/R \cap H \cong E/H \cong \prod_{\mathfrak{m}} S.$$

So $r_S(R) \geq \mathfrak{m}$. But obviously $w_0(R) \leq \mathfrak{m}$. Thus $r_S(R) = \mathfrak{m}$, as desired. □

8.8 The Congruence Kernel of $\mathbf{SL_2(Z)}$

Recall (see Section 4.7) that the congruence kernel K of $\mathrm{SL}_2(\mathbf{Z})$ is the kernel of the natural continuous epimorphism

$$\varphi : \widehat{\mathrm{SL}_2(\mathbf{Z})} \longrightarrow \mathrm{SL}_2(\widehat{\mathbf{Z}}) \cong \prod_p \mathrm{SL}_2(\mathbf{Z}_p).$$

The following theorem describes K and, in particular, it shows that φ is not an isomorphism, i.e., that the profinite topology of $\mathrm{SL}_2(\mathbf{Z})$ is strictly finer than its congruence subgroup topology.

Theorem 8.8.1 *The congruence kernel K of $\mathrm{SL}_2(\mathbf{Z})$ is a free profinite group of countably infinite rank.*

Proof. The group $\mathrm{SL}_2(\mathbf{Z})$ can be expressed as an amalgamated product

$$\mathrm{SL}_2(\mathbf{Z}) = \langle a \rangle *_{\langle c \rangle} \langle b \rangle,$$

where

$$a = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad b = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad c = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = a^2 = b^3$$

(cf., for example, Serre [1980], Example I.4.2(c)).

Consider the congruence subgroup $\Gamma_2(3)$, that is, the kernel of the natural epimorphism

$$\psi : \mathrm{SL}_2(\mathbf{Z}) \longrightarrow \mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z}).$$

Note that $\Gamma_2(3)$ has finite index in $\mathrm{SL}_2(\mathbf{Z})$ and $\Gamma_2(3) \cap \langle a \rangle = \Gamma_2(3) \cap \langle b \rangle = 1$. Hence, $\Gamma_2(3)$ is a free abstract group of finite rank (cf. Serre [1980], Proposition I.18). Since $\langle c \rangle$ is a finite central subgroup of $\mathrm{SL}_2(\mathbf{Z})$, we have that $\langle c \rangle$ is a central subgroup of $\widehat{\mathrm{SL}_2(\mathbf{Z})}$. Let $\varphi_p : \widehat{\mathrm{SL}_2(\mathbf{Z})} \longrightarrow \mathrm{SL}_2(\mathbf{Z}_p)$ be the continuous epimorphism induced by φ. Clearly $\varphi_p(\langle c\rangle)$ is a subgroup of order 2 which is central in $\mathrm{SL}_2(\mathbf{Z}_p)$. Since $\widehat{\mathrm{SL}_2(\mathbf{Z})}/K \cong \mathrm{SL}_2(\widehat{\mathbf{Z}}) \cong \prod_p \mathrm{SL}_2(\mathbf{Z}_p)$, we have that $\widehat{\mathrm{SL}_2(\mathbf{Z})}/K$ contains an infinite closed central subgroup L of exponent 2.

Since $\Gamma_2(3)$ is an abstract free group of finite rank, $\widehat{\Gamma_2(3)}$ is a free profinite group of the same rank (see Proposition 3.3.6). The group $\widehat{\Gamma_2(3)}$ can be identified with the closure of $\Gamma_2(3)$ in $\widehat{\mathrm{SL}_2(\mathbf{Z})}$ because $\Gamma_2(3)$ has finite index in $\mathrm{SL}_2(\mathbf{Z})$; moreover, it is clear that $\widehat{\Gamma_2(3)} \geq K$. Since $\widehat{\Gamma_2(3)}/K$ is open in $\widehat{\mathrm{SL}_2(\mathbf{Z})}/K$, we have that $(\widehat{\Gamma_2(3)}/K) \cap L \neq 1$. Hence $\widehat{\Gamma_2(3)}/K$ contains a normal subgroup R/K of order 2, where $K \triangleleft_o R \triangleleft_c \widehat{\Gamma_2(3)}$. Therefore, $d(R) = \aleph_0$ by Proposition 8.5.10. Thus, Theorem 8.7.1 implies that K is a free profinite group of rank $\aleph_0$. □

8.9 Sufficient Conditions for Freeness

The criterion of freeness for normal subgroups of free pro-$\mathcal{C}$ groups given in Theorem 8.6.8 is sometimes difficult to use in practice. So it is convenient to have other sufficient conditions of freeness that one can verify more easily. To give such conditions is the purpose of this section. Sufficient conditions for freeness have already appeared in Theorems 8.4.2 and 8.4.3 and in Corollary 8.4.4. Our first result is a very useful test for freeness for certain "verbal" subgroups of a free pro-$\mathcal{C}$ group.

Theorem 8.9.1 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}$ on a basis X converging to 1. Assume that $\Phi = \Phi(X)$ is the subgroup of F generated by X as an abstract group. Let $N \triangleleft_c F$. If $N \cap \Phi \neq 1$, then N is a free pro-$\mathcal{C}$ group.*

Proof. By Theorem 3.6.2, we may assume that N is of infinite index in F. Note that if $\mathfrak{m} = 1$, then $\Phi \cong \mathbf{Z}$; hence $N = \overline{N \cap \Phi}$ has finite index in F. Therefore, we may also assume that $\mathfrak{m} \geq 2$. Let S be a finite simple group. By Proposition 8.6.2, $r_S(N) = \mathfrak{m}^*$, where $\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$. Thus the result follows from Theorem 8.6.8. □

Let G be a profinite group. Its n-th *derived subgroup* $G^{(n)}$ $(n = 0, 1, 2, \dots)$ is defined recursively by

$$G^{(0)} = G,\ \ G^{(n+1)} = \overline{[G^{(n)}, G^{(n)}]}.$$

The series

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(n)} \geq \cdots$$

is termed the *derived series* of G. The group $G^{(1)}$ is also called the *commutator subgroup* of G, and often denoted by G'.

Similarly, recall (see Exercise 2.3.17) that the n-th term $G_n = \gamma_n(G)$ $(n = 1, 2, \dots)$ of the lower central series

$$G = G_1 \geq G_2 \geq \cdots \geq G_n \geq \cdots$$

of G is defined recursively by

$$G_1 = G, \qquad G_{n+1} = \overline{[G, G_n]}.$$

As examples of how to make use of the test for freeness of Theorem 8.9.1, we list explicitly some types of subgroups of a free pro-$\mathcal{C}$ group for which freeness is preserved.

Corollary 8.9.2 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group. Then the following closed subgroups of F are also free pro-$\mathcal{C}$ groups.*

(a) *The n-th derived group $F^{(n)}$ of F $(n = 0, 1, \dots)$;*
(b) *The n-th term F_n of the lower central series of F $(n = 1, 2, \dots)$.*

Corollary 8.9.3 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let N be a closed normal subgroup of a free pro-$\mathcal{C}$ group $F = F_{\mathcal{C}}(\mathfrak{m})$ of rank $\mathfrak{m} \geq 2$ such that F/N is abelian. Then N is a free pro-$\mathcal{C}$ group.*

Proof. We use the notation of the theorem above. Since F/N is abelian, it follows that $N \geq [F, F]$. Hence $N \cap \Phi(X) \neq \emptyset$ ($\Phi(X)$ is the abstract free group on X). So the result is a consequence of Theorem 8.9.1. □

The next result sharpens Theorem 8.4.2.

Theorem 8.9.4 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Assume that N and K are closed normal subgroups of F such that $N < K \triangleleft F$ and $d(K/N) < d(K)$. Then N is a free pro-$\mathcal{C}$ group.*

Proof. By Theorems 3.6.2, 8.7.1 and 8.4.2, we may assume that $[F : K]$ and $[K : N]$ are both infinite. Then $d(K) = \mathfrak{m}^*$ according to Theorem 8.6.5. Choose a proper open normal subgroup L of K containing N; then L is free pro-$\mathcal{C}$ of rank $\mathfrak{m}^*$ by Theorem 8.7.1. If $d(L/N)$ is finite, then obviously $d(L/N) < d(L)$. On the other hand, if $d(L/N)$ is infinite (see Corollary 2.6.3 and Corollary 3.6.3),

$$d(L/N) = w_0(L/N) = w_0(K/N) = d(K/N) < d(K) = \mathfrak{m}^* = d(L).$$

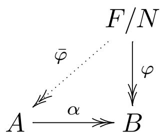
Thus, applying Theorem 8.4.2 to the subgroup N of L, one deduces that N is free pro-$\mathcal{C}$, as asserted. □

Lemma 8.9.5 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of infinite rank $\mathfrak{m}$ and let N be a closed normal subgroup of F. Assume that the set*

$$\Delta = \{S \in \mathcal{C} \mid S \text{ is a simple group and } r_S(N) < \mathfrak{m}\}$$

is nonempty, and let $\mathcal{C}(\Delta)$ be the class of all finite Δ-groups (see Section 2.1). Then,

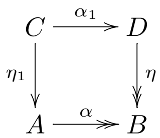
(a) *An embedding problem of the form*



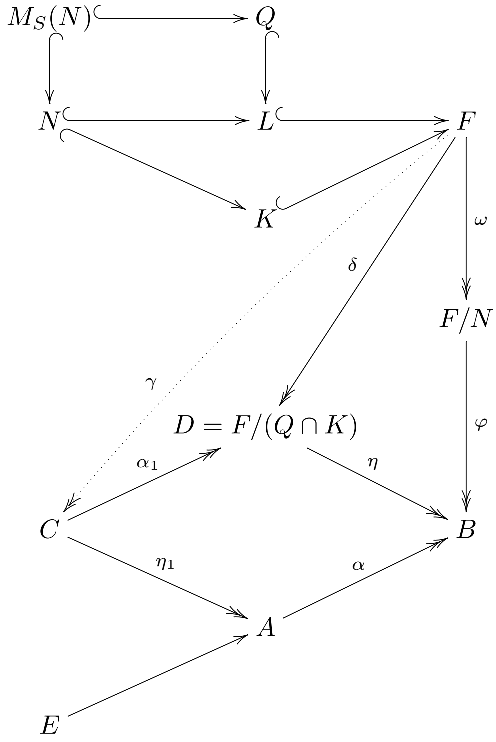
is solvable whenever A and B are pro-$\mathcal{C}$ groups such that $w_0(B) < \mathfrak{m}$, $w_0(A) \leq \mathfrak{m}$ and $\mathrm{Ker}(\alpha)$ is a pro-$\mathcal{C}(\Delta)$ group.

(b) *If $S \in \Delta$, then $r_S(F/N) = \mathfrak{m}$.*

Proof. (a) We need to construct a continuous epimorphism $\bar{\varphi} : F/N \longrightarrow A$ such that $\alpha\bar{\varphi} = \varphi$. By Lemma 3.5.4, we may assume that $E = \mathrm{Ker}(\alpha)$ is a finite minimal normal subgroup of A. By the minimality of $E = \mathrm{Ker}(\alpha)$, we must have that $E = \prod S$ (a finite direct product of copies of S), for some $S \in \Delta$ (for, if $S \in \Delta$ is involved in E, then $M_S(E) \triangleleft_c A$). By Lemma 8.3.8, there exist closed normal subgroups L and Q of F with $M_S(N) \triangleleft_c Q \triangleleft_c L$ and $N \triangleleft_c L$ such that $L/M_S(N) = N/M_S(N) \times Q/M_S(N)$ and $w_0(F/L) \leq w_0(N/M_S(N))$. Hence $Q \cap N = M_S(N)$. Since, by assumption, $w_0(N/M_S(N)) < \mathfrak{m}$, we have $w_0(F/Q) < \mathfrak{m}$. Let $\mathrm{Ker}(\varphi) = K/N$, where $N \leq K \triangleleft F$. Denote by $\omega : F \longrightarrow F/N$ and $\delta : F \longrightarrow D = F/Q \cap K$ the canonical epimorphisms. Let $\eta : D \longrightarrow B$ be the epimorphism defined by $\eta(f(Q \cap K)) = \varphi(fN)$ $(f \in F)$. Clearly $\eta\delta = \varphi\omega$. Consider the pullback (see Section 2.10)



of α and η. We shall think of C as consisting of those pairs $(a, d) \in A \times D$ such that $\alpha(a) = \eta(d)$. Since α and η are epimorphisms, so are α_1 and η_1.



Note that $w_0(F/K) = w_0(B) < \mathfrak{m}$. Since D can be embedded in the group $F/Q \times F/K$ and C can be embedded in $A \times D$, we have $w_0(D) < \mathfrak{m}$ and $w_0(C) \le \mathfrak{m}$. Then, according to Theorem 3.5.9, there exists an epimorphism

$$\gamma : F \longrightarrow C$$

such that $\alpha_1\gamma = \delta$. Since $\delta(N) \le \mathrm{Ker}(\eta)$, one has

$$\gamma(N) \le \alpha_1^{-1}(\delta(N)) = E \times \delta(N).$$

Claim: $(\eta_1\gamma)(N) = 1$.

Case 1. S is nonabelian.

Observe that

$$\delta(N) = N(Q \cap K)/Q \cap K \cong N/M_S(N).$$

Hence $E \times \delta(N)$ is a direct product of copies of S. Since $\gamma(N)$ is a normal subgroup of $E \times \delta(N)$, it follows that $\gamma(N) = E_1 \times \delta(N)$, for some subgroup E_1 of E. Since $\delta(N) \cong N/M_S(N)$ is the largest quotient of N which is a direct product of copies of S, it follows that $E_1 = 1$. Thus $(\eta_1\gamma)(N) = 1$ in this case.

Case 2. $S = C_p$, for some prime p.

Since $r_p(N) < \mathfrak{m}$, we have $r_p(N) = 0$ (see Theorem 8.6.11). So $M_p(N) = N$, and hence $Q = F$; therefore $Q \cap K = K$. Then $\delta(N) = 1$. If $\gamma(N) \neq 1$, we would have that $\gamma(N) = E \times \delta(N)$ has a quotient isomorphic to C_p. Therefore, $r_p(N) \geq 1$, a contradiction. Thus $\gamma(N) = 1$, and hence the claim is proved.

From the claim we deduce that $\eta_1\gamma$ induces an epimorphism

$$\bar{\varphi} : F/N \longrightarrow A.$$

Then $\alpha\bar{\varphi} = \varphi$, as needed.

(b) First observe that $r_S(F/N) > 0$. Indeed, if $r_S(F/N) = 0$, then $NM_S(F) = F$; hence $N/N \cap M_S(F) \cong F/M_S(F)$. Therefore, $r_S(N) = \mathfrak{m}$, a contradiction. It follows that there exists a continuous epimorphism $\varphi : G/N \longrightarrow S$. Choose a projection map $\alpha : \prod_{\mathfrak{m}} S \longrightarrow S$. By part (a), φ can be lifted to an epimorphism $\bar{\varphi} : G/N \longrightarrow \prod_{\mathfrak{m}} S$. Thus, $r_S(F/N) \geq \mathfrak{m}$. □

Theorem 8.9.6 *Let $\mathcal{C}$ be an NE-formation of finite groups. Let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of infinite rank $\mathfrak{m}$ and let N be a closed normal subgroup of F. Assume that the set*

$$\Delta = \{S \in \mathcal{C} \mid S \textit{ is a simple group and } r_S(N) < \mathfrak{m}\}$$

is nonempty, and let

$$R = \bigcap \{H \mid N \leq H \triangleleft_o F, F/H \textit{ is a pro-}\mathcal{C}(\Delta) \textit{ group}\},$$

where $\mathcal{C}(\Delta)$ is the class of all finite Δ-groups (see Section 2.1). Then F/R is a free pro-$\mathcal{C}(\Delta)$ group of rank $\mathfrak{m}$.

Proof. Let $S \in \Delta$. By Lemma 8.9.5(b), there is a continuous epimorphism $G/N \longrightarrow \prod_{\mathfrak{m}} S$. Remark that every continuous epimorphism $F/N \longrightarrow A$ onto a pro-$\mathcal{C}(\Delta)$ group A factors through the canonical epimorphism $F/N \longrightarrow F/R$. Hence, there exists a continuous epimorphism

$$F/R \longrightarrow \prod_{\mathfrak{m}} S.$$

Thus, $w_0(G/R) = \mathfrak{m}$. So, by Theorem 3.5.9, it suffices to prove that F/R has the strong lifting property over the class $\mathcal{E}$ of all epimorphisms of pro-$\mathcal{C}(\Delta)$ groups. From the remark above, it suffices to prove that F/N has the strong lifting property over $\mathcal{E}$. This follows from Lemma 8.9.5(a). □

Theorem 8.9.7 *Let $\mathcal{C}$ be an NE-formation of finite groups and let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Suppose that K_1 and K_2 are closed normal subgroups of F such that neither of them contains the other. Then $N = K_1 \cap K_2$ is a free pro-$\mathcal{C}$ group.*

Proof. By Theorem 8.7.1, we may assume that $[F : K_i] = \infty$ $(i = 1, 2)$. Choose L_i to be a proper open normal subgroup of K_i containing N $(i = 1, 2)$; then L_1 and L_2 are both free pro-$\mathcal{C}$ by Theorem 8.7.1. Clearly $L_1 \cap L_2 = N$. One easily checks that $L_i \triangleleft K_1K_2$ $(i = 1, 2)$; it follows that L_1L_2 is a proper open normal subgroup of K_1K_2. So, by Theorem 8.7.1, L_1L_2 is a free pro-$\mathcal{C}$ group. Hence, replacing K_i by L_i $(i = 1, 2)$ and F by L_1L_2, we may assume that $F = K_1K_2$, and that K_1 and K_2 are free pro-$\mathcal{C}$ nontrivial normal subgroups of infinite index.

Suppose first that the rank $\mathfrak{m}$ of F is finite. Since $F/N \cong K_1/N \times K_2/N$, the group F/N does not satisfy Schreier's formula (see Lemma 8.4.5). Therefore N is free pro-$\mathcal{C}$ by Corollary 8.4.4.

Assume now that the rank $\mathfrak{m}$ of F is infinite. Consider the family

$$\varDelta = \{S \in \mathcal{C} \mid S \text{ is a simple group and } r_S(N) < \mathfrak{m}\}.$$

If $\varDelta$ is empty, then N is free pro-$\mathcal{C}$ of rank $\mathfrak{m}$ by Theorem 8.6.8. Suppose that $\varDelta$ is nonempty. Put $\mathcal{C}' = \mathcal{C}(\varDelta)$, the class of all finite $\varDelta$-groups, (see Section 2.1) and let

$$R = \bigcap\{H \mid N \leq H \triangleleft_o F, F/H \text{ is a pro-}\mathcal{C}' \text{ group}\}.$$

Then, by Theorem 8.9.6, $\bar{F} = F/R$ is a free pro-$\mathcal{C}'$ group of rank $\mathfrak{m}$. Let $\varphi : F \longrightarrow \bar{F}$ be the canonical epimorphism and let $\bar{K}_i = \varphi(K_i) = K_iR/R$ $(i = 1, 2)$. Since $R \geq N$, φ factors through F/N. From

$$F/N = K_1/N \times K_2/N$$

we deduce that $\bar{K}_1 \cap \bar{K}_2$ is in the center of $\bar{F}$. By Corollary 8.7.3, $\bar{K}_1 \cap \bar{K}_2 = 1$, and, by Proposition 8.7.7, this implies that either $\bar{K}_1$ or $\bar{K}_2$ is trivial. Say $\bar{K}_1 = 1$, i.e., $K_1R = R$. Then $K_1 \leq R$. Hence, $F = RK_2$ and so F/K_2 has no quotients belonging to $\varDelta$. Let $S \in \varDelta$. Since the free pro-$\mathcal{C}$ group K_1 is a normal nontrivial subgroup of F, its rank is $\mathfrak{m}$ (see Theorem 8.6.8). Therefore, we have $K_1/M_S(K_1) \cong \prod_{\mathfrak{m}} S$. Now,

$$K_1/M_S(K_1)N \cong F/M_S(K_1)K_2 = 1$$

since $K_1/M_S(K_1)N$ is a direct product of copies of S (see Lemma 8.2.4) and, as we have pointed out before, S is not a quotient of F/K_2. Therefore, $K_1 = M_S(K_1)N$. So,

$$N/(M_S(K_1) \cap N) \cong K_1/M_S(K_1) \cong \prod_{\mathfrak{m}} S.$$

Thus $r_S(N) = \mathfrak{m}$. This is a contradiction since $S \in \varDelta$. So $\varDelta = \emptyset$, and $N = K_1 \cap K_2$ is free pro-$\mathcal{C}$, as asserted. $\square$

Corollary 8.9.8 *Let $\mathcal{C}$ be an NE-formation of finite groups and let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of rank $\mathfrak{m} \geq 2$. Suppose*

$$\varphi : F \longrightarrow G_1 \times G_2$$

is a continuous epimorphism, where G_1 and G_2 are nontrivial pro-$\mathcal{C}$ groups. Then Ker(φ) is a free pro-$\mathcal{C}$ group.

Proof. Denote by $\pi_i : G_1 \times G_2 \longrightarrow G_i$ $(i = 1, 2)$ the canonical projections. Then $\mathrm{Ker}(\pi_1\varphi)$ and $\mathrm{Ker}(\pi_2\varphi)$ are nontrivial and

$$\mathrm{Ker}(\varphi) = \mathrm{Ker}(\pi_1\varphi) \cap \mathrm{Ker}(\pi_2\varphi).$$

So the result follows from the theorem above. □

The following theorem is in some sense a counterpart to Theorem 8.7.1 in the case of free groups of finite rank.

Theorem 8.9.9 *Let $\mathcal{C}$ be an NE-formation of finite groups and let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of finite rank $\mathfrak{m} \geq 2$. Suppose that N is a closed normal subgroup of F of infinite index. Then, there exists $H \triangleleft_c F$ such that $N \leq H$ and H is a free pro-$\mathcal{C}$ group of countably infinite rank.*

Proof. Denote by $\varDelta$ the subset of $\mathcal{C}$ consisting of those simple groups S for which $r_S(N)$ is finite. Observe that if $\varDelta = \emptyset$, then N itself is free pro-$\mathcal{C}$ by Theorem 8.6.8; in this case we can take $H = N$.

Suppose then that $\varDelta \neq \emptyset$, and let $S \in \varDelta$. Consider an open normal subgroup K of F containing N whose rank k as a free pro-$\mathcal{C}$ group satisfies $r_S(F_{\mathcal{C}}(k-1)) > r_S(N)$. Let X be a basis of F, and let $\varPhi$ be the abstract group generated by X. By Proposition 3.3.13, $\varPhi$ is a free abstract group. Since $K \triangleleft_o F$, $\varPhi \cap K$ is a free abstract group of rank k. Let Y be a basis of $\varPhi \cap K$, and let $y \in Y$. Denote by L the closed normal subgroup of K generated by y. Clearly K/L is a free pro-$\mathcal{C}$ group of rank $k-1$. We claim that the index of NL in K is infinite. Indeed, otherwise NL/L is a free pro-$\mathcal{C}$ group of rank $n \geq k-1$ (see Theorem 3.6.2). So, using Lemmas 8.2.5 and 8.2.7, we have

$$r_S(N) \geq r_S(F_{\mathcal{C}}(n)) \geq r_S(F_{\mathcal{C}}(k-1)) > r_S(N),$$

a contradiction. Choose a set $\{t_i \mid i = 1, \ldots, r\}$ of coset representatives of K in F belonging to $\varPhi$. Then

$$W = \bigcap_{i=1}^{r} L^{t_i}$$

is a normal subgroup of F. It follows that $W \cap \varPhi \neq 1$. Put $H = NW$. Observe that the index of H in F is infinite, for $H \leq NL$. Therefore, by Theorems 8.6.5 and 8.9.1, H is free pro-$\mathcal{C}$ of rank $\aleph_0$. □

Exercise 8.9.10 Let S be a fixed finite simple group and let $\mathcal{C}$ be the class of all finite S-groups (see Section 2.1). Assume that $F = F_{\mathcal{C}}(\mathfrak{m})$ is a free pro-$\mathcal{C}$ group of infinite rank $\mathfrak{m}$. Let $N \triangleleft_c F$. Then either N or F/N is a free pro-$\mathcal{C}$ group.

8.10 Characteristic Subgroups of Free Pro-$\mathcal{C}$ Groups

In Section 8.5 we characterized those homogeneous groups that can be realized as normal subgroups of free pro-$\mathcal{C}$ groups. In this section we describe the homogeneous groups with the more restrictive property that they can be realized as characteristic subgroups of free pro-$\mathcal{C}$ groups.

Lemma 8.10.1 *Let $\mathcal{C}$ be a formation of finite groups and let F be a free pro-$\mathcal{C}$ group. Let U, V be closed normal subgroups of F and let $\beta : F/U \longrightarrow F/V$ be a continuous isomorphism. Then if either the rank of F is finite or the rank of F is infinite and both U and V are open subgroups, then β is induced by an automorphism α of F, i.e., $\alpha(U) = V$ and $\beta(tU) = \alpha(t)V$, for each $t \in F$.*

Proof. This is equivalent to proving the existence of an automorphism α of F such that the diagram

$$\begin{array}{ccc} F & \xrightarrow{\alpha} & F \\ {\scriptstyle \pi_U}\downarrow & & \downarrow{\scriptstyle \pi_V} \\ F/U & \xrightarrow[\beta]{} & F/V \end{array}$$

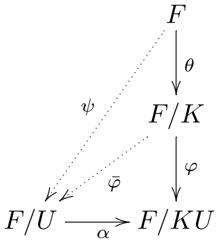
commutes, where the vertical maps are the natural projections. If the rank of F is infinite, this follows from Theorem 3.5.9 and Proposition 3.5.6. Assume that rank(F) is finite and let $\{x_1, \dots, x_n\}$ be a basis of F. By Proposition 2.5.4, there are elements $y_1, \dots, y_n \in F$ such that $\pi_V(y_i) = \beta\pi_U(x_i)$ ($i = 1, \dots, n$) and $F = \overline{\langle y_1, \dots, y_n \rangle}$. Let $\alpha : F \longrightarrow F$ be the epimorphism defined by $\alpha(x_i) = y_i$ ($i = 1, \dots, n$). Clearly $\pi_V\alpha = \beta\pi_U$. Finally, by Proposition 2.5.2, α is an isomorphism. □

Theorem 8.10.2 *Let $\mathcal{C}$ be an NE-formation of finite groups and let $F = F_{\mathcal{C}}(\mathfrak{m})$ be a free pro-$\mathcal{C}$ group of infinite rank $\mathfrak{m}$.*

(a) *If K is a closed characteristic subgroup of F, then $r_S(K)$ equals 0 or $\mathfrak{m}$ for every finite simple group S.*
(b) *Assume that $\Delta \subseteq \Sigma_{\mathcal{C}}$. Then there exists a characteristic subgroup K of F for which $r_S(K) > 0$ (and thus, $r_S(K) = \mathfrak{m}$) if and only if $S \in \Delta$.*

Proof. (a) Let K be a characteristic subgroup of F and let S be a finite simple group with $r_S(K) \neq 0$. Then $M_S(K) \triangleleft_c F$. By Proposition 2.1.4, there exists an open normal subgroup U of F such that $M_S(K) \leq K \cap U < K$. Hence $KU/U \cong K/K \cap U \cong \prod S$, a finite direct product of copies of S.

Suppose that $r_S(K) < \mathfrak{m}$. Consider the diagram



where α, θ and φ are the canonical epimorphisms. By Lemma 8.9.5, there exists a continuous epimorphism $\bar{\varphi} : F/K \longrightarrow F/U$ such that $\alpha\bar{\varphi} = \varphi$. Define $\psi : F \longrightarrow F/U$ by $\psi = \bar{\varphi}\theta$. Then $K \leq \mathrm{Ker}(\psi)$. Let $\bar{\psi} : F/\mathrm{Ker}(\psi) \longrightarrow F/U$ be the isomorphism induced by ψ. By Lemma 8.10.1, there exists a continuous automorphism $\beta : F \longrightarrow F$ lifting $\bar{\psi}$. Since K is characteristic, one has $K = \beta(K) \leq \beta(\mathrm{Ker}(\psi)) = U$. This, however, contradicts the fact that, by construction, $K \cap U < K$. Hence $r_S(K) = \mathfrak{m}$.

(b) If $\Delta = \Sigma_{\mathcal{C}}$, one can put $K = F$. Let $\Delta \neq \Sigma_{\mathcal{C}}$. Set $\Gamma = \Sigma - \Delta$ and let $\mathcal{C}' = \mathcal{C}(\Gamma)$ (see Section 2.1). Define $K = R_{\mathcal{C}'}(F)$ (see Section 3.4). Hence K is characteristic. By Lemma 3.4.1, $r_S(K) = 0$ for each $S \in \Gamma$. On the other hand, if $S \in \Delta$, there exists some $U \triangleleft_o F$ such that $F/U \cong S$. Note that $U \not\geq K$ since $S \notin \mathcal{C}'$. So, $KU = F$. Hence $K/K \cap U \cong F/U \cong S$. Thus, $r_S(K) > 0$. □

The next goal of this section is to describe characteristic subgroups of a free profinite group in terms of formations of finite groups. This gives additional useful information about characteristic subgroups.

Let G be a profinite group and let $\mathcal{C}$ be a formation of finite groups. It follows from Lemma 3.4.1 that the subgroup $R_{\mathcal{C}}(G)$ of G is characteristic; furthermore, if $\mathcal{C}$ is a variety of finite groups, then $R_{\mathcal{C}}(G)$ is fully invariant. From the definition of $R_{\mathcal{C}}(G)$ one can see that these subgroups play a role analogous to that of verbal subgroups in the theory of abstract groups. If $F = F(\mathfrak{m})$ is a free profinite group of rank $\mathfrak{m}$ and $\mathcal{C}$ is a formation of profinite groups, then the quotient group $F/R_{\mathcal{C}}(F)$ is a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}$.

In the abstract theory of group varieties, the bijection between varieties and fully invariant subgroups of free groups plays an important role. In the context of profinite groups, this extends to a correspondence between formations and characteristic subgroups of free profinite groups, as we see in the following

Theorem 8.10.3 *Let F be a free profinite group of infinite rank. Then the map $\mathcal{C} \longrightarrow R_{\mathcal{C}}(F)$ defines a bijective correspondence between the set of all formations of finite groups and the set of characteristic subgroups of F. Moreover, $\mathcal{C}$ is a variety if and only if $R_{\mathcal{C}}(G)$ is fully invariant in F.*

Proof. Let K be a characteristic subgroup of F. Denote by $\mathcal{C}$ the class of all finite groups which are quotient groups of F/K. We show that $\mathcal{C}$ is a formation of profinite groups. To do this, it suffices to prove that $\mathcal{C}$ is closed under taking quotient groups and subdirect products of a finite collection of groups. The first of these is clear. To prove the second, assume that G is a finite group and let $N_i \triangleleft G$ be such that $G/N_i \cong G_i \in \mathcal{C}$ $(i = 1, 2)$ and $N_1 \cap N_2 = 1$. We have to show that $G \in \mathcal{C}$. Since the rank of F is infinite, there exists an epimorphism $\varphi : F \longrightarrow G$. Put $V_i = \varphi^{-1}(N_i)$, $i = 1, 2$. Then $V_1 \cap V_2 = \mathrm{Ker}(\varphi)$. By the definition of $\mathcal{C}$, there exist open normal subgroups W_1 and W_2 of F such that $K \le W_i$ and $F/W_i \cong G_i \cong F/V_i$ $(i = 1, 2)$. By Lemma 8.10.1, there exist automorphisms α_1, α_2 of F such that $\alpha_i(W_i) = V_i$, $i = 1, 2$. Since K is characteristic, $K = \alpha_i(K) \le \alpha(W_i) = V_i$. It follows that $K \le \mathrm{Ker}(\varphi) = V_1 \cap V_2$; therefore $G \in \mathcal{C}$.

Next we show that $K = R_{\mathcal{C}}(G)$. Let M be a closed normal subgroup of F such that F/M is a pro-$\mathcal{C}$ group. Then $F/U \in \mathcal{C}$ for any open normal subgroup U of F containing M. It follows from the definition of $\mathcal{C}$ that there exists an open normal subgroup V of F such that $K \le V$ and $F/V \cong F/U$. By Lemma 8.10.1, there exists an automorphism α of F such that $\alpha(V) = U$. Hence $K = \alpha(K) \le \alpha(V) = U$. It follows that $K \le R_{\mathcal{C}}(F)$. The reverse inclusion is obvious since F/K is pro-$\mathcal{C}$.

One deduces from Lemma 3.4.1 that $R_{\mathcal{C}}(F)$ is characteristic (respectively, fully invariant) if $\mathcal{C}$ is formation (respectively, a variety) of finite groups. It remains to show that if $R_{\mathcal{C}}(F)$ is fully invariant, then $\mathcal{C}$ is a variety. To do this we have to prove that $\mathcal{C}$ is closed under taking subgroups. Let $G \in \mathcal{C}$ and assume that H is a subgroup of G. By definition of $\mathcal{C}$, there exists an epimorphism $\psi : F \longrightarrow G$ such that $\mathrm{Ker}(\psi)$ contains K. Put $V = \psi^{-1}(H)$. Since $w_0(V) \le w_0(F) = \mathrm{rank}(F)$, there exists an epimorphism $\eta : F \longrightarrow V$ (see Theorem 3.5.9) which we can regard as an endomorphism of F. Since $\eta(K) \le K \le \mathrm{Ker}(\psi)$, the group $H \cong V/\mathrm{Ker}(\psi)$ is an epimorphic image of F/K and therefore belongs to $\mathcal{C}$. $\square$

Next we state a result that generalizes Proposition 4.5.4. We shall give only a brief sketch of the proof, which is based in part on Theorem 8.10.3.

Theorem 8.10.4 *Let K be a characteristic subgroup of a free profinite group F. Then every automorphism of the quotient group F/K can be lifted to an automorphism of F.*

If the rank of F is finite, this result was proved as part of Proposition 5.4.4. Suppose that the rank of F is infinite. Then, by Theorem 8.10.3, $K = R_{\mathcal{C}}(F)$ for some formation $\mathcal{C}$ of finite groups. Then, the idea of the proof is to prove analogs of Lemma 8.5.6 and Proposition 8.5.7 after replacing $M(-)$ by $R_{\mathcal{C}}(-)$ at appropriate places. For an explicit proof of this theorem see Mel'nikov [1982].

8.11 Notes, Comments and Further Reading

The main idea for Theorem 8.1.3 appears in Gildenhuys and Lim [1972]. This chapter is based mainly on work of O.V. Mel'nikov. Most of the results and the methods contained here can be traced back to his papers, specially Mel'nikov [1976, 1978, 1982, 1988]. In most cases our presentation is somewhat more general than his.

The concept of a group 'satisfying Schreier's formula' is due to Lubotzky and van den Dries [1981]; they use it to give an elegant and independent proof of Theorem 8.7.9 when F is at most countably generated.

Theorem 8.7.9, in the form presented here, appears in Jarden and Lubotzky [1992]. Theorem 8.4.7 appears in Lubotzky [1982] (the analog of this theorem for abstract free groups is also valid, and it was proved by R. Strebel). Versions of 8.7.2–8.7.5 appear in Gruenberg [1967] (where a version of Corollary 8.7.5 is attributed to O. Kegel), Anderson [1974], Mel'nikov [1978], Oltikar and Ribes [1978], Lubotzky and van den Dries [1981]. Theorem 8.9.7 is due to Jarden and Lubotzky [1992].

Further results of this type have been proved by Haran [1999] and Bary-Soroker [2006]. Combining their results, they prove:

Theorem 8.11.1 *Let $F = F(\mathfrak{m})$ be a free profinite group of rank $\mathfrak{m} \geq 2$. Suppose that N is a closed subgroup of F of infinite index and K_1 and K_2 are closed normal subgroups of F such that $N \geq K_1 \cap K_2$ but $K_i \not\leq N$ $(i = 1, 2)$. Then N is a free profinite group of rank* $\max\{\aleph_0, \mathfrak{m}\}$.

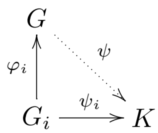
9 Free Constructions of Profinite Groups

Throughout this chapter $\mathcal{C}$ denotes a variety of finite groups.

In this chapter we introduce free products, free products with amalgamation and HNN-extensions in the category of pro-$\mathcal{C}$ groups. We shall study only basic properties of these constructions here.

9.1 Free Pro-$\mathcal{C}$ Products

In this section we study free pro-$\mathcal{C}$ products of finitely many pro-$\mathcal{C}$ groups. Let G_i $(i = 1, \ldots, n)$ be a finite collection of pro-$\mathcal{C}$ groups. A free *pro-$\mathcal{C}$ product* of these groups consists of a pro-$\mathcal{C}$ group G and continuous homomorphisms $\varphi_i : G_i \longrightarrow G$ $(i = 1, \ldots, n)$ satisfying the following universal property:



for any pro-$\mathcal{C}$ group K and any continuous homomorphisms $\psi_i : G_i \longrightarrow K$ $(i = 1, \ldots, n)$, there is a unique continuous homomorphism $\psi : G \longrightarrow K$ such that $\psi_i = \psi\varphi_i$ for all $i = 1, \ldots, n$. We refer to ψ as the homomorphism *induced* by the ψ_i, and we refer to the φ_i as the *canonical maps* of the free pro-$\mathcal{C}$ product.

We denote a free pro-$\mathcal{C}$ product of the groups $G_1, \ldots, G_n$ by

$$G = \coprod_{i=1}^{n} G_i \quad \text{or by} \quad G = G_1 \amalg \cdots \amalg G_n.$$

This is justified because free products are unique in a certain natural sense (see Proposition 9.1.2).

Observe that one needs to test the above universal property only for finite groups $K \in \mathcal{C}$, for then it holds automatically for any pro-$\mathcal{C}$ group K, since K is an inverse limit of groups in $\mathcal{C}$.

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4_9,

Exercise 9.1.1

(a) Let $G = A * B$ be a free product of abstract groups. Prove that $G_{\hat{\mathcal{C}}} = A_{\hat{\mathcal{C}}} \amalg B_{\hat{\mathcal{C}}}$. (Hint: use Corollary 3.1.6 and the universal property.)
(b) Prove that a free pro-$\mathcal{C}$ group of finite rank is a free pro-$\mathcal{C}$ product of copies of $\mathbf{Z}_{\hat{\mathcal{C}}}$.

Proposition 9.1.2 *Let $\{G_i \mid i = 1, \dots, n\}$ be a collection of pro-$\mathcal{C}$ groups. Then there exists a unique free pro-$\mathcal{C}$ product*

$$G = \coprod_{i=1}^{n} G_i.$$

Proof. The meaning of 'uniqueness' in this context is the following: assume that G, together with continuous homomorphisms $\varphi_i : G_i \longrightarrow G$ is a free pro-$\mathcal{C}$ product of the groups $\{G_i \mid i = 1, \dots, n\}$, and assume that $\tilde{G}$, together with continuous homomorphisms $\tilde{\varphi}_i : G_i \longrightarrow \tilde{G}$ is another free pro-$\mathcal{C}$ product of the groups $\{G_i \mid i = 1, \dots, n\}$; then there exists a unique continuous isomorphism $\rho : G \longrightarrow \tilde{G}$ such that $\rho\varphi_i = \tilde{\varphi}_i$, for all $i = 1, \dots, n$. From the universal property in the definition of free product it is easily deduced that if a free pro-$\mathcal{C}$ product exists, then it is unique.

To prove the existence we give an explicit construction of

$$G = \coprod_{i=1}^{n} G_i.$$

Let $G^{abs} = G_1 * \cdots * G_n$ be a free product of $G_1, \dots, G_n$ considered as abstract groups. Denote by $\varphi_i^{abs} : G_i \longrightarrow G^{abs}$ the natural embeddings. Let

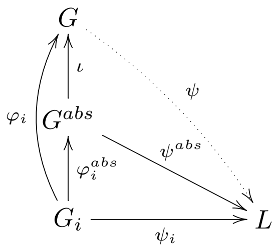
$$\mathcal{N} = \{N \triangleleft_f G^{abs} \mid (\varphi_i^{abs})^{-1}(N) \triangleleft_o G_i \text{ for all } i = 1, \dots, n \text{ and } G^{abs}/N \in \mathcal{C}\}.$$

One easily checks that $\mathcal{N}$ is filtered from below (see Section 3.2). Define $G = \mathcal{K}_{\mathcal{N}}(G^{abs})$ to be the completion of G^{abs} with respect to the topology determined by $\mathcal{N}$ (see Section 3.2). Denote by

$$\iota : G^{abs} \longrightarrow G$$

the natural homomorphism and put $\varphi_i = \iota\varphi_i^{abs}$. Then each φ_i is continuous. We show that G and φ_i $(i = 1, \dots, n)$ satisfy the universal property of a free product.

Let $\psi_i : G_i \longrightarrow L$, $(i = 1, \dots, n)$ be continuous homomorphisms to some group $L \in \mathcal{C}$. Then, by the universal property for abstract free products, there exists a unique homomorphism $\psi^{abs} : G^{abs} \longrightarrow L$ with $\psi_i = \psi^{abs}\varphi_i^{abs}$. It follows that $(\varphi_i^{abs})^{-1}(\mathrm{Ker}(\psi^{abs})) = \mathrm{Ker}(\psi_i)$ is open in G_i for every $i = 1, \dots, n$. Since $L \in \mathcal{C}$ one has that $\mathrm{Ker}(\psi^{abs}) \in \mathcal{N}$. Therefore (see Lemma 3.2.1), there exists a continuous homomorphism $\psi : G \longrightarrow L$ with $\psi^{abs} = \psi\iota$. Thus the following diagram



is commutative. This implies that $\psi_i = \psi\varphi_i$. Since $G = \mathcal{K}_{\mathcal{N}}(G^{abs})$, one has that

$$G = \overline{\langle \varphi_i(G_i) \mid i = 1, \ldots, n \rangle}$$

from where the uniqueness of ψ follows. □

Remark 9.1.3 Think of the G_i as being embedded in

$$G^{abs} = G_1 * \cdots * G_n.$$

Then $G = G_1 \amalg \cdots \amalg G_n$ is the completion of G^{abs} with respect to the topology defined by the collection of all normal subgroups N of finite index in G^{abs} such that $N \cap G_i$ is open in G_i $(i = 1, \ldots, n)$ and $G^{abs}/N \in \mathcal{C}$.

Corollary 9.1.4 *Let $G_1, \ldots, G_n$ be pro-$\mathcal{C}$ groups and let $G = G_1 \amalg \cdots \amalg G_n$ be their free pro-$\mathcal{C}$ product. Then*

(a) *the natural homomorphisms*

$$\varphi_j : G_j \longrightarrow G = \coprod_{i=1}^{n} G_i \quad (j = 1, \ldots, n)$$

are monomorphisms; *and*

(b) $G = \overline{\langle \varphi_i(G_i) \mid i = 1, \ldots, n \rangle}$.

Proof. Part (b) follows from the explicit construction of a free pro-$\mathcal{C}$ product given in the proof of Proposition 9.1.2.

(a) Fix j. Define $\psi_j : G_j \longrightarrow G_j$ to be the identity map and $\psi_i : G_i \longrightarrow G_j$ to be the trivial homomorphism for $i \neq j$ $(i = 1, \ldots, n)$. Let $\psi : G \longrightarrow G_j$ be the homomorphism induced by $\psi_1, \ldots, \psi_n$. Then $\psi\varphi_j = \mathrm{id}_{G_j}$. Therefore, φ_j is injective. □

Terminology: If $H \leq_c G$ are pro-$\mathcal{C}$ groups and there exists a closed subgroup K of G such that $G = H \amalg K$, then we say that H is a *free factor* of G (as pro-$\mathcal{C}$ groups).

Let $\mu_i : G_i \longrightarrow H_i$ $(i = 1, 2)$ be continuous homomorphisms of pro-$\mathcal{C}$ groups. Denote by

$$\mu_1 \amalg \mu_2 : G_1 \amalg G_2 \longrightarrow H_1 \amalg H_2$$

the unique continuous homomorphism that makes the following diagrams commutative ($i = 1, 2$)

$$\begin{array}{ccc} G_1 \amalg G_2 & \xrightarrow{\mu_1 \amalg \mu_2} & H_1 \amalg H_2 \\ \uparrow & & \uparrow \\ G_i & \xrightarrow[\mu_i]{} & H_i \end{array}$$

where the vertical maps are the canonical monomorphisms.

In the next result we show that the operations of taking inverse limits and free pro-$\mathcal{C}$ products commute.

Lemma 9.1.5 *Let* $\{G_{1i}, \mu_{1ij}, I_1\}$ *and* $\{G_{2i}, \mu_{2ij}, I_2\}$ *be surjective inverse systems of pro-*$\mathcal{C}$ *groups over posets* I_1 *and* I_2*, respectively. Then,*

(a) $I_1 \times I_2$ *is a poset in a natural way and* $\{G_{1i} \amalg G_{2k}, \mu_{1ij} \amalg \mu_{2kr}, I_1 \times I_2\}$ *is an inverse system over* $I_1 \times I_2$.

(b)
$$\left(\varprojlim_{I_1} G_{1i}\right) \amalg \left(\varprojlim_{I_2} G_{2i}\right) \cong \varprojlim_{I_1 \times I_2} (G_{1i} \amalg G_{2k}).$$

Proof. Part (a) is straightforward. We indicate the main steps to prove part (b). Set

$$G_1 = \varprojlim_{I_1} G_{1i}, \qquad G_2 = \varprojlim_{I_1} G_{2i} \quad \text{and} \quad G = \varprojlim_{I_1 \times I_2} (G_{1i} \amalg G_{2k}),$$

and denote by

$$\mu_{1i} : G_1 \to G_{1i}, \qquad \mu_{2k} : G_2 \to G_{1ki} \quad \text{and}$$
$$\mu_{ik} : G \to G_{1i} \amalg G_{2k} \quad (i \in I_1, k \in I_2)$$

the projection maps.

For $(i, k) \in I_1 \times I_2$, consider the composition

$$G_1 \xrightarrow{\mu_{1i}} G_{1i} \longrightarrow G_{1i} \amalg G_{2k}$$

of canonical homomorphisms. These maps are compatible, and induce a corresponding continuous homomorphism

$$\varphi_1 : G_1 \longrightarrow G = \varprojlim_{I_1 \times I_2} (G_{1i} \amalg G_{2k}).$$

In an analogous way we obtain a continuous homomorphism $\varphi_2 : G_2 \longrightarrow G$. To prove the lemma, it suffices to show that G together with the maps φ_1 and φ_2 is a free pro-$\mathcal{C}$ product of G_1 and G_2. Remark that from our definitions it follows easily that G is topologically generated by $\varphi_1(G_1)$ and $\varphi_2(G_2)$.

Let K be a group in $\mathcal{C}$ and let $\psi_i : G_i \longrightarrow K$ $(i = 1, 2)$ be continuous homomorphisms. We have to prove that there is a continuous homomorphism $\psi : G \longrightarrow K$ such that $\psi\varphi_i = \psi_i$ $(i = 1, 2)$. Observe that such ψ, if it exists, would be unique by the remark just made. To define ψ we proceed as follows. By Lemma 1.1.16, there exist indices $j_i \in I_i$ such that ψ_i factors through G_{ij_i} $(i = 1, 2)$, i.e., there are continuous homomorphisms $\rho_i : G_{ij_i} \longrightarrow K$ $(i = 1, 2)$ such that

$$\psi_i = \rho_i \mu_{ij_i} \quad (i = 1, 2).$$

Let $\rho : G_{1j_1} \amalg G_{1j_2} \longrightarrow K$ be the continuous homomorphism induced by ρ_1 and ρ_2. Define $\psi : G \longrightarrow K$ to be the composition

$$G \stackrel{\mu_{j_1 j_2}}{\longrightarrow} G_{j_1} \amalg G_{j_2} \stackrel{\rho}{\longrightarrow} K$$

of the natural projection and ρ. One checks readily that ψ satisfies the required conditions. $\square$

Let $G = G_1 \coprod G_2$ be a free pro-$\mathcal{C}$ product of pro-$\mathcal{C}$ groups G_1 and G_2. Denote by $\psi_i : G_i \longrightarrow G_1 \times G_2$ $(i = 1, 2)$ the natural inclusions. Then, by the universal property, the maps ψ_i induce a continuous homomorphism

$$\psi : G \longrightarrow G_1 \times G_2.$$

The kernel of ψ is called the *cartesian subgroup* of G (there is a certain abuse of language here, since the cartesian kernel depends on the chosen decomposition of G as a free product). Our next theorem gives a description of the cartesian subgroup of G that mirrors the situation in free products of abstract groups.

Theorem 9.1.6 *Let $\mathcal{C}$ be an extension closed variety of finite groups and let $G = G_1 \amalg G_2$ be a free pro-$\mathcal{C}$ product of pro-$\mathcal{C}$ groups G_1 and G_2. Then the cartesian subgroup K of G is a free pro-$\mathcal{C}$ group on the pointed profinite space* $(\{[g_1, g_2] \mid g_1 \in G_1, g_2 \in G_2\}, 1)$, *where* $[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2$.

Proof. Suppose first that G_1 and G_2 are finite. Then K is open in G. It follows that K is the pro-$\mathcal{C}$ completion of the cartesian subgroup K^{abs} of the abstract free product $G_1 * G_2$ (see Lemmas 3.1.4 and 3.2.6). It is known (see Serre [1980], Proposition I.4) that K^{abs} is a free abstract group with basis

$$\{[g_1, g_2] \mid g_1 \in G_1 - \{1\}, g_2 \in G_2 - \{1\}\}.$$

So, by Proposition 3.3.6, K is a free pro-$\mathcal{C}$ group on the finite space

$$\{[g_1, g_2] \mid g_1 \in G_1 - \{1\}, g_2 \in G_2 - \{1\}\}.$$

Therefore, the result is proved in this case.

Assume now that G_1 and G_2 are arbitrary pro-$\mathcal{C}$ groups. Represent G as an inverse limit of groups $G_{NM} = G_1/N \amalg G_2/M$, where N and M

run through the open normal subgroups of G_1 and G_2 respectively (see Lemma 9.1.5). Clearly, then $K = \varprojlim_{M,N} K_{MN}$ is the inverse limit of the cartesian subgroups K_{MN} of G_{MN}. Moreover, the canonical epimorphism $G_{MN} \longrightarrow G_{M'N'}$ ($N \leq N'$, $M \leq M'$) map the pointed basis of K_{MN} described above onto the corresponding pointed basis of $K_{M'N'}$. Hence the result follows from Proposition 3.3.9. □

Corollary 9.1.7 *Let $\mathcal{C}$ be an extension closed variety of finite groups and let $G = G_1 \amalg G_2$ be a free pro-$\mathcal{C}$ product of pro-$\mathcal{C}$ groups G_1 and G_2. Then for any closed subgroups $H_1 \leq G_1$ and $H_2 \leq G_2$, the free pro-$\mathcal{C}$ product $H = H_1 \amalg H_2$ is canonically embedded in $G = G_1 \amalg G_2$.*

Proof. Consider the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K_G & \longrightarrow & G = G_1 \amalg G_2 & \xrightarrow{\varphi} & G_1 \times G_2 & \longrightarrow & 1 \\ & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} & & {\scriptstyle \gamma}\uparrow & & \\ 1 & \longrightarrow & K_H & \longrightarrow & H = H_1 \amalg H_2 & \xrightarrow{\psi} & H_1 \times H_2 & \longrightarrow & 1 \end{array}$$

with exact rows (φ and ψ send free factors identically to the corresponding direct factors). By Theorem 9.1.6 K_G and K_H are free pro-$\mathcal{C}$ on the pointed profinite spaces

$$(\{[g_1, g_2] \mid g_1 \in G_1, g_2 \in G_2\}, 1) \quad \text{and} \quad (\{[h_1, h_2] \mid h_1 \in H_1, h_2 \in H_2\}, 1),$$

respectively. The map β is induced by the inclusions $H_i \longrightarrow G_i$ ($i = 1, 2$), and α and γ are given by $\alpha([h_1, h_2]) = [h_1, h_2]$, $\gamma(h_1, h_2) = (h_1, h_2)$ ($h_1 \in H_1, h_2 \in H_2$). Clearly γ is a monomorphism. By Lemma 3.3.11, α is a monomorphism as well. Hence so is β. □

Proposition 9.1.8 *Let $\mathcal{C}$ be an extension closed variety of finite groups and let $G_1, \dots, G_n$ be pro-$\mathcal{C}$ groups. Let $G^{abs} = G_1 * \cdots * G_n$ be the abstract free product of the groups $G_1, \dots, G_n$. Then the natural homomorphism*

$$\iota : G^{abs} = G_1 * \cdots * G_n \longrightarrow G = G_1 \amalg \cdots \amalg G_n$$

is a monomorphism.

Proof. Recall that if $g \in G^{abs} = G_1 * \cdots * G_n$ is nontrivial, then it can be written uniquely as $g = x_1 x_2 \cdots x_m$, where $m \geq 1$, $x_j \in (\bigcup_{i=1}^n G_i) - \{1\}$ and where $x_j \in G_i$ implies $x_{j+1} \notin G_i$ for all $j = 1, \dots, m-1$ (see, for example, Serre [1980]). We need to prove that $\iota(g) \neq 1$. For every $1 \leq i \leq n$ let $\psi_i : G_i \longrightarrow H_i$ be a continuous epimorphism onto a group $H_i \in \mathcal{C}$ such that $\psi_i(x_j) \neq 1$, whenever $x_j \in G_i$. Let $H = H_1 \amalg \cdots \amalg H_n$ be the corresponding free pro-$\mathcal{C}$ product. By Corollary 9.1.4(a), we can think of H_i as subgroups of H. By the universal property (of G), the maps ψ_i induce a continuous homomorphism

$$\psi : G \longrightarrow H = \coprod_{i=1}^{n} H_i.$$

Since each ψ_i is onto, one deduces from Corollary 9.1.4(b) that ψ is an epimorphism. It suffices to prove that $\psi\iota(g) \neq 1$.

Let $H^{abs} = H_1 * \cdots * H_n$ be the free product of the groups $H_1, \ldots, H_n$, as abstract groups. We claim that H^{abs} is residually $\mathcal{C}$. Indeed, let K^{abs} be the cartesian subgroup of H^{abs} (i.e., the kernel of the epimorphism $H^{abs} \longrightarrow H_1 \times \cdots \times H_n$ that sends each H_i identically to its canonical copy in $H_1 \times \cdots \times H_n$). Then K^{abs} is open in the pro-$\mathcal{C}$ topology of H^{abs}. By the Kurosh subgroup theorem for abstract groups (see Serre [1980], Theorem I.14 and the exercise following that theorem), K^{abs} is a free abstract group of finite rank. By Lemma 3.1.4(a) the topology induced on K^{abs} from the pro-$\mathcal{C}$ topology of H^{abs} coincides with the full pro-$\mathcal{C}$ topology on K^{abs}. Hence it is enough to show that K^{abs} is residually $\mathcal{C}$. The latter follows from Proposition 3.3.15. This proves the claim.

Since all H_i are finite, we have $H = (H^{abs})_{\hat{\mathcal{C}}}$ by Exercise 9.1.1(a) (alternatively, use the construction of pro-$\mathcal{C}$ products in the proof of Proposition 9.1.2). So, by the claim above, the canonical homomorphism $H^{abs} \longrightarrow H$ is a monomorphism. It follows that we can think of H^{abs} as a dense subgroup of H. Then $\psi\iota(g) = \psi_{i_1}(x_1) \cdots \psi_{i_m}(x_m)$, where i_j is the index of the free factor containing x_j and the latter product is taken inside of H^{abs}. Since the maps ψ_{i_j} were chosen in such a way that $\psi_{i_j}(x_j) \neq 1$ for all $j = 1, \ldots, m$, one has that $\psi\iota(g) = \psi_{i_1}(x_1) \cdots \psi_{i_m}(x_m) \neq 1$ and the result follows. □

Next we prove a pro-$\mathcal{C}$ version of the Kurosh subgroup theorem for open subgroups of free pro-$\mathcal{C}$ products of pro-$\mathcal{C}$ groups. There is no pro-$\mathcal{C}$ analog of the Kurosh subgroup theorem for general closed subgroups of such products.

Theorem 9.1.9 *Let $\mathcal{C}$ be an extension closed variety of finite groups and let $G_1, \ldots, G_n$ be a finite collection of pro-$\mathcal{C}$ groups. Let D be an open subgroup of the free pro-$\mathcal{C}$ product $G = G_1 \amalg \cdots \amalg G_n$. Then D is a free pro-$\mathcal{C}$ product*

$$D = \coprod_{i=1}^{n} \coprod_{\tau \in D\backslash G/G_i} (D \cap g_{i,\tau} G_i g_{i,\tau}^{-1}) \amalg F, \tag{1}$$

where

(a) *for each i, $g_{i,\tau}$ ranges over a system of double coset representatives for $D\backslash G/G_i$ containing* 1; *and*
(b) *F is a free pro-$\mathcal{C}$ group of rank* $1 + (n-1)[G:D] - \sum_{i=1}^{n} |D\backslash G/G_i|$.

Proof. Let $\Gamma = G^{abs} = G_1 * \cdots * G_n$ be the abstract free product of the G_i. By Proposition 9.1.8, we can think of Γ as a dense subgroup of G. Put $\Delta = D \cap \Gamma$. By the Kurosh subgroup theorem for abstract groups

$$\Delta = \left[\mathop{\ast}_{i=1}^{n} \mathop{\ast}_{\tau \in \Delta \backslash \Gamma / G_i} (\Delta \cap g_{i,\tau} G_i g_{i,\tau}^{-1}) \right] \ast \Phi,$$

where, for each i, $g_{i,\tau}$ ranges over a system of double cosets representatives for $\Delta\backslash\Gamma/G_i$ containing 1, and where Φ is a free abstract group of rank

$$1 + (n-1)[\Gamma : \Delta] - \sum_{i=1}^{n} |\Delta\backslash\Gamma/G_i|$$

(see Serre [1980], Theorem I.14 and Exercise 2 following that theorem). We remark that

(1) $\Delta \cap g_{i,\tau} G_i g_{i,\tau}^{-1} = D \cap g_{i,\tau} G_i g_{i,\tau}^{-1}$ for all $g_{i,\tau}$ and all $i = 1, \dots, n$; and
(2) since D is open, the double cosets in $D\backslash G/G_i$ are just the topological closures of the double cosets in $\Delta\backslash\Gamma/G_i$. Hence, for each i,

$$\{g_{i,\tau} \mid \tau \in \Delta\backslash\Gamma/G_i\}$$

is also a system of double coset representatives for $D\backslash G/G_i$.

Let $\mathcal{N}$ be the collection of all normal subgroups N of Γ of finite index such that $N \cap G_i$ is open in G_i for all $i = 1, \dots, n$, and $G/N \in \mathcal{C}$. Denote by $\mathcal{T}_{\mathcal{N}}$ the topology on Γ defined by $\mathcal{N}$. According to Remark 9.1.3, G is the completion of Γ with respect to the topology $\mathcal{T}_{\mathcal{N}}$.

Denote by $\mathcal{T}$ the topology on Δ induced by $\mathcal{T}_{\mathcal{N}}$. By Corollary 9.1.4(a), the topology of each G_i as a profinite group coincides with the topology induced by $\mathcal{T}_{\mathcal{N}}$. It follows that the topology of each $D \cap g_{i,\tau} G_i g_{i,\tau}^{-1}$ as a profinite group coincides with the topology induced by $\mathcal{T}_{\mathcal{N}}$.

Define $\mathcal{M}$ to be the collection of all normal subgroups M of Δ of finite index such that $M \cap D \cap g_{i,\tau} G_i g_{i,\tau}^{-1}$ is open in $D \cap g_{i,\tau} G_i g_{i,\tau}^{-1}$ and $\Phi/M \cap \Phi \in \mathcal{C}$. Then $\mathcal{M}$ determines a second topology $\mathcal{T}_{\mathcal{M}}$ on Δ such that the groups in $\mathcal{M}$ are a fundamental system of neighborhoods of 1.

We claim that $\mathcal{T} = \mathcal{T}_{\mathcal{M}}$. Clearly $\mathcal{T}$ is coarser than $\mathcal{T}_{\mathcal{M}}$. To show the converse, it suffices to prove that if $M \in \mathcal{M}$, then there exists some $N \in \mathcal{N}$ with $N \le M$. To do this we first follow the argument used in the proof of Lemma 3.1.4(a) to construct a subgroup of finite index in M which is normal in Γ: consider the core M_Γ of M in Γ. Put $K = \Delta_\Gamma \cap M$, and note that $K_\Gamma = M_\Gamma$. Then, as in that lemma, $\Delta_\Gamma/M_\Gamma \in \mathcal{C}$ and $\Gamma/\Delta_\Gamma \in \mathcal{C}$; since $\mathcal{C}$ is extension closed and since the group Γ/M_Γ is an extension of Δ_Γ/M_Γ by Γ/Δ_Γ, we obtain that $\Gamma/M_\Gamma \in \mathcal{C}$. Put $N = M_\Gamma$.

To see that $N \in \mathcal{N}$, we still need to verify that $N \cap G_i$ is open in G_i $(i = 1, \dots, n)$. Note that $N = \bigcap_{j=1}^{t} \gamma_j^{-1} M \gamma_j$, where $\gamma_1, \dots, \gamma_t$ is a (finite) set of representatives of the right cosets of M in Γ. Therefore, to prove that $N \cap G_i$ is open in G_i, it suffices to prove that for any $\gamma \in \Gamma$, $\gamma^{-1} M \gamma \cap G_i$ is open in G_i; or, equivalently, that $M \cap \gamma G_i \gamma^{-1}$ is open in $\gamma G_i \gamma^{-1}$. Say $\gamma \in \Delta g_{i,\tau} G_i$; then $\gamma = \delta g_{i,\tau} g_i$, for some $\delta \in \Delta$, $g_i \in G_i$. So it suffices to prove that $M \cap \delta g_{i,\tau} G_i g_{i,\tau}^{-1} \delta^{-1}$ is open in $\delta g_{i,\tau} G_i g_{i,\tau}^{-1} \delta^{-1}$. Since M is normal in Δ, this is equivalent to showing that $M \cap g_{i,\tau} G_i g_{i,\tau}^{-1}$ is open in $g_{i,\tau} G_i g_{i,\tau}^{-1}$. But this is the case because $M \in \mathcal{M}$, $M \cap g_{i,\tau} G_i g_{i,\tau}^{-1} = M \cap D \cap g_{i,\tau} G_i g_{i,\tau}^{-1}$ and D is open. This proves the claim.

Therefore, D is the completion of Δ with respect to the topology $\mathcal{T}_{\mathcal{M}}$. It is immediate from the definition of $\mathcal{M}$, that $\mathcal{T}_{\mathcal{M}}$ induces on the free group Φ its full pro-$\mathcal{C}$ topology. Hence the closure F of Φ in D coincides with the pro-$\mathcal{C}$ completion of Φ. Thus (see Proposition 3.3.6), F is a free pro-$\mathcal{C}$ group of rank

$$1 + (n-1)[\Gamma : \Delta] - \sum_{i=1}^{n} |\Delta \backslash \Gamma / G_i| = 1 + (n-1)[G : D] - \sum_{i=1}^{n} |D \backslash G / G_i|,$$

where the equality holds since $\Delta = D \cap \Gamma$ and D is open in G.

To finish the proof that the decomposition (1) holds, we show that the appropriate universal property of free pro-$\mathcal{C}$ products is satisfied. Let $H \in \mathcal{C}$ and let $f_{i,\tau} : D \cap g_{i,\tau} G_i g_{i,\tau}^{-1} \longrightarrow H$ $(i = 1, \dots, n;\ \tau \in D \backslash G / G_i)$ and $f : F \longrightarrow H$ be continuous homomorphisms. Let $\varphi : \Phi \longrightarrow H$ be the restriction of f to Φ. Then, the maps $f_{i,\tau}$ and φ induce a homomorphism

$$\psi : \Delta = \left[\ast_{i=1}^{n} \ast_{\tau \in D \backslash \Gamma / G_i} (D \cap g_{i,\tau} G_i g_{i,\tau}^{-1}) \right] \ast \Phi \longrightarrow H.$$

Observe that ψ is continuous if we endow Δ with the topology $\mathcal{T}_{\mathcal{M}}$. Indeed, if $K = \mathrm{Ker}(\phi)$, then obviously $\Delta / K \in \mathcal{C}$ and $\Phi / K \cap \Phi \in \mathcal{C}$; furthermore, $K \cap D \cap g_{i,\tau} G_i g_{i,\tau}^{-1}$ is open in $D \cap g_{i,\tau} G_i g_{i,\tau}^{-1}$ since it coincides with $\mathrm{Ker}(f_{i,\tau})$, which is open by the continuity of $f_{i,\tau}$.

Therefore, ψ extends to a unique continuous homomorphism on the completion D of Δ with respect to $\mathcal{T}_{\mathcal{M}}$ (see Lemma 3.2.1)

$$\bar{\psi} : D \longrightarrow H,$$

and obviously $\bar{\psi}$ extends the maps $f_{i,\tau}$ and f uniquely. □

Corollary 9.1.10 *Under the assumptions of the theorem above, one has that $H \cap G_i$ is a free factor of H for every $i = 1, \dots, n$.*

Next proposition shows that in contrast with the situation for abstract groups, a free factor of a free pro-$\mathcal{C}$ group is not necessarily a free pro-$\mathcal{C}$ group.

Proposition 9.1.11 *Let F be a free pro-$\mathcal{C}$ group of infinite rank $\mathfrak{m}$ and let P be a projective pro-$\mathcal{C}$ group with local weight $w_0(P) \le w_0(F)$. Then the free pro-$\mathcal{C}$ product $G = F \amalg P$ is isomorphic to F.*

Proof. By Theorem 3.5.9, it suffices to show the strong lifting property for G over the class $\mathcal{E}$ of all epimorphisms of pro-$\mathcal{C}$ groups. Consider the $\mathcal{E}$-embedding problem

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \stackrel{\alpha}{\longrightarrow} & B & \longrightarrow & 1 \end{array}$$

with $w_0(B) < w_0(G)$ and $w_0(A) \leq w_0(G)$. We must show that there exists a continuous epimorphism $\bar{\varphi} : G \longrightarrow A$ such that $\alpha\bar{\varphi} = \varphi$. Note that $w_0(F) = w_0(G)$. Since F is free pro-$\mathcal{C}$, there exists a continuous epimorphism $\varphi_0 : F \longrightarrow \alpha^{-1}(\varphi(F))$ such that $\alpha\varphi_0 = \varphi_{|F}$. Since P is projective, there exists a continuous homomorphism $\varphi_1 : P \longrightarrow A$ such that $\alpha\varphi_1 = \varphi_{|P}$. By the universal property of free pro-$\mathcal{C}$ products, φ_0 and φ_1 induce a continuous homomorphism $\bar{\varphi} : G \longrightarrow A$ such that $\alpha\bar{\varphi} = \varphi$. It remains to prove that $\bar{\varphi}$ is an epimorphism. Since $K \leq \bar{\varphi}(G)$, one has $\bar{\varphi}(G) = \alpha^{-1}(\alpha(\bar{\varphi}(G))) = \alpha^{-1}(\varphi(G)) = \alpha^{-1}(B) = A$. □

Theorem 9.1.12 *Let $G_1, \ldots, G_n$ be pro-$\mathcal{C}$ groups and let $G = G_1 \amalg \cdots \amalg G_n$ be their free pro-$\mathcal{C}$ product. Then $G_i \cap G_i^x = 1$ for $x \in G - G_i$. In particular one has $N_G(G_i) = G_i$ and $C_G(a) = C_{G_i}(a)$ for $a \in G_i$ $(i = 1, \ldots, n)$.*

Proof. Fix $i \in \{1, \ldots, n\}$ and let $x \in G - G_i$. Choose an open normal subgroup U of G such that $x \notin G_iU$. Then by Theorem 9.1.9, G_iU admits a Kurosh decomposition

$$G_iU = \coprod_{j=1}^{n} \coprod_{\tau \in G_iU\backslash G/G_j} (G_iU \cap G_j^{g_{j,\tau}}) \amalg F, \tag{2}$$

where

(1) for each j, $g_{j,\tau}$ ranges over a system of double cosets representatives containing 1 for $G_iU\backslash G/G_j$, and
(2) F is a free pro-$\mathcal{C}$ group.

Since $x \notin G_iU$, there exists some $g_{i,\tau} \neq 1$ such that $x = g_i g_{i,\tau} g_i' u$, for some $g_i, g_i' \in G_i$, $u \in U$, because U is normal. Note that G_i appears as one of the free factors in the decomposition (2), namely $G_iU \cap G_i = G_i$. On the other hand, $G_i^x = G_i^{g_{i,\tau} g_i' u}$. Let

$$\psi : G_iU \longrightarrow \prod_{j=1}^{n} \prod_{\tau \in G_iU\backslash G/G_j} (G_iU \cap G_j^{g_{j,\tau}}) \times F$$

be the homomorphism induced by the maps that send each free factor in (2) identically to the corresponding direct factor of the direct product. Now,

$$G_i \cap G_i^x = G_i \cap G_iU \cap G_i^x = G_i \cap (G_iU \cap G^{g_{i,\tau} g_i' u}).$$

Hence,

$$\begin{aligned}&\psi(G_i \cap G_i^x)\\&\quad \leq \psi(G_i) \cap \psi(G_i U \cap G^{g_{i,\tau} g_i' u})\\&\quad = \psi(G_i) \cap \psi((G_i U \cap G^{g_{i,\tau}})^{g_i' u}) = \psi(G_i) \cap \psi(G_i U \cap G^{g_{i,\tau}}) = 1.\end{aligned}$$

Thus $G_i \cap G_i^x = 1$, since ψ is an injective map when restricted to

$$G_i U \cap G^{g_{i,\tau} g_i' u} = (G_i U \cap G^{g_{i,\tau}})^{g_i' u}. \qquad \square$$

In the next proposition we describe the maximal abelian subgroups of a free profinite group.

Proposition 9.1.13 *Let F be a nonabelian free profinite group and let π be a set of primes. Then $\mathbf{Z}_{\hat{\pi}} = \prod_{p\in\pi} \mathbf{Z}_p$ is isomorphic to a maximal abelian closed subgroup of F.*

Proof. First we assume that F has infinite rank. By Proposition 9.1.11, $F = H \amalg A$, where $H \cong F$ and $A \cong \mathbf{Z}_{\hat{\pi}}$. Hence, by Theorem 9.1.12, A is self-normalized, and hence maximal abelian.

Suppose now that F is of finite rank ≥ 2. Choose $p \in \pi$. Let $\varphi : F \longrightarrow \mathbf{Z}_p$ be an epimorphism and N the kernel of φ. By Corollary 8.9.3 and Theorem 8.6.11, N is a free profinite group of countable rank. By the case above, there exists a maximal abelian closed subgroup A of N with $A \cong \mathbf{Z}_{\hat{\pi}}$. To prove that A is a maximal abelian closed subgroup of F it suffices to show that A is self-centralized in F. Suppose on the contrary that there exists $x \in F - N$ centralizing A. Then x centralizes also the p-Sylow subgroup $A_p \cong \mathbf{Z}_p$ of A. By our choice of φ and N, the Sylow p-subgroup $\overline{\langle x\rangle}_p$ of $\overline{\langle x\rangle}$ is nontrivial. Hence

$$\overline{\langle A_p, \overline{\langle x\rangle}_p\rangle} \cong \mathbf{Z}_p \times \mathbf{Z}_p$$

is a subgroup of F. However, $cd_p(\mathbf{Z}_p \times \mathbf{Z}_p) = 2$ and $cd_p(F) = 1$, a contradiction (see Exercise 7.4.3 and Corollary 7.5.3). $\square$

Next we give an example to show that an inverse limit of free profinite groups is not necessarily free (see Theorem 3.5.15).

Example 9.1.14 Let F be a free profinite group of infinite countable rank and let P be a free pro-p group of rank $2^{\aleph_0}$. Let $G = F \amalg P$ be their free profinite product. Choose a decomposition

$$P = \varprojlim P_i$$

such that each P_i is a free pro-p quotient group of P of finite rank (see Corollary 3.3.10). Let $\{P_i, \varphi_{ij}\}$ be the corresponding inverse system. Define an inverse system $\{F \amalg P_i, \psi_{ij}\}$ where ψ_{ij} is induced by id_F and φ_{ij}. Then

$$G = \varprojlim (F \amalg P_i)$$

by Lemma 9.1.5. By Proposition 9.1.11, $F \amalg P_i$ is a free profinite group of countable rank for every i.

On the other hand, G is not free profinite. One can see this as follows. First note that $w_0(G) = 2^{\aleph_0}$. Let q be a prime number different from p, and let Q be a free pro-q group of rank $2^{\aleph_0}$. Let $\rho : P \longrightarrow B$ be a continuous epimorphism onto a certain finite p-group B. Consider a diagram

$$\begin{array}{ccc} & & G = F \amalg P \\ & & \Big\downarrow{\scriptstyle \varphi} \\ Q \times P & \xrightarrow{\ \alpha\ } & B \end{array}$$

where φ is induced by ρ and the trivial map $F \longrightarrow B$, and α is the composition of the natural projection $Q \times P \longrightarrow P$ and the map ρ. It is clear that φ cannot be lifted (if $\bar{\varphi} : G \longrightarrow Q \times P$ is an epimorphism, then $F \longrightarrow G \longrightarrow Q \times P \longrightarrow Q$ would be an epimorphism; this would contradict the assumptions on the ranks of F and Q). Thus, G is not free profinite (see Theorem 3.5.9).

We turn to the study of free pro-p products. Assume that $G_1, \ldots, G_n$ are pro-p groups and let $G = G_1 \amalg \cdots \amalg G_n$ be their free pro-p product. Corollary 9.1.4 allows us to identify each G_i with its canonical image in G.

The Grushko-Neumann theorem which is a deep result for free products of abstract groups is very easy to prove in the pro-p case. We do this in the next

Proposition 9.1.15 *Let $G = G_1 \amalg G_2$ be a free pro-p product of pro-p groups G_1 and G_2. Then $d(G) = d(G_1) + d(G_2)$.*

Proof. By Corollary 9.1.4(b), G is generated by G_1 and G_2. So $d(G) \leq d(G_1) + d(G_2)$. On the other hand, $G_1 \times G_2$ is a quotient of G and so is $A = G_1/\Phi(G_1) \times G_2/\Phi(G_2)$. The last group is just an elementary abelian p-group (see Lemma 2.8.7(b)) with

$$d(A) = d(G_1/\Phi(G_1)) + d(G_2/\Phi(G_2)) = d(G_1) + d(G_2).$$

Thus $d(G) \geq d(G_1) + d(G_2)$. □

Remark 9.1.16 The corresponding question for free profinite of profinite groups has a negative answer (see Section 9.5 for details), that is, if $G = G_1 \amalg G_2$ is the free profinite product of two profinite groups G_1 and G_2, one may have $d(G) \neq d(G_1) + d(G_2)$.

Lemma 9.1.17 *Let A and B be pro-p groups.*

(a) *Let $G = A \amalg B$ (free pro-p product). Then the Frattini subgroups of G and B are related as follows:*

$$\Phi(B) = B \cap \Phi(G).$$

(b) *Let $G = A \times B$. Then $\Phi(B) = B \cap \Phi(G)$.*
(c) *Let G be defined as either in (a) or in (b). Then $G/\Phi(G)$ is naturally isomorphic to $A/\Phi(A) \times B/\Phi(B)$.*

Proof. The proof of parts (a) and (b) is formally the same. In both cases we think of A and B as subgroups of G. By Lemma 2.8.7(c), $\Phi(B) \le B \cap \Phi(G)$. To prove the other inclusion, consider the natural epimorphism

$$\varphi : G \longrightarrow B \longrightarrow B/\Phi(B).$$

By Lemma 2.8.7(c), $\Phi(G) \le \mathrm{Ker}(\varphi)$. On the other hand, if $x \in B - \Phi(B)$, then $x \notin \mathrm{Ker}(\varphi)$, and so $x \notin \Phi(G)$. Thus, $B \cap \Phi(G) \le \Phi(B)$.

We leave the proof of (c) to the reader. □

The following lemma gives an easy criterion for a subgroup of a free pro-p group to be a free factor.

Lemma 9.1.18 *Let F be a free pro-p group and let H be a closed subgroup of F. Then the following two conditions are equivalent:*

(a) *H is a free factor of F, i.e., there exists a closed subgroup M of F such that $F = H \amalg M$ (free pro-p product);*
(b) *$\Phi(F) \cap H = \Phi(H)$.*

Proof. The implication (a) $\Longrightarrow$ (b) follows from Lemma 9.1.17. Assume now that (b) holds. From the inclusion $H \longrightarrow F$, we may assume that $H/\Phi(H)$ is embedded in $F/\Phi(F)$. So, by Proposition 2.8.16, $F/\Phi(F) = H/\Phi(H) \times V$, where V is a closed subgroup of $F/\Phi(F)$. Let $\varphi : F \longrightarrow F/\Phi(F)$ be the canonical epimorphism. By Lemma 2.8.15, there exists a minimal closed subgroup M of F such that $\varphi(M) = V$ and $\mathrm{Ker}(\varphi_{|M}) \le \Phi(M)$. Hence $M \cap \Phi(F) \le \Phi(M)$, and so $M \cap \Phi(F) = \Phi(M)$.

Define $G = H \amalg M$ to be the free pro-p product of H and M. Let $\psi : G \longrightarrow F$ be the homomorphism induced by the inclusions $H, M \longrightarrow F$. Then ψ is surjective, since the induced map $\bar{\psi} : G/\Phi(G) \longrightarrow F/\Phi(F)$ is an isomorphism by Lemma 9.1.17(c). Now, ψ has a right inverse $\alpha : F \longrightarrow G$, since F is a free pro-p group. However, α is also surjective since the induced map $\bar{\alpha} : F/\Phi(F) \longrightarrow G/\Phi(G)$ coincides with $(\bar{\psi})^{-1}$, which is an isomorphism. Thus ψ is an isomorphism. □

The previous lemma can be used to proof a pro-p analog of a well known theorem of M. Hall.

Theorem 9.1.19 *Let H be a finitely generated closed subgroup of a free pro-p group F. Then H is a free factor of some open subgroup L of F.*

Proof. By Proposition 2.1.4(d),

$$H = \bigcap_{H \le H_i \le_o F} H_i.$$

Then, by Proposition 2.8.9,

$$\Phi(H) = \bigcap_{H \le H_i \le_o F} \Phi(H_i).$$

It follows that $\Phi(H) = \bigcap_{H \le H_i \le_o F}(H \cap \Phi(H_i))$. Since H is finitely generated, $\Phi(H)$ is open in H. Hence, there exists H_{i_0} such that $\Phi(H) = H \cap \Phi(H_{i_0})$. Lemma 9.1.18 applies now to yield that H is a free factor of H_{i_0}. □

Now we are in a position to prove a pro-p version of Howson's theorem Howson [1954].

Theorem 9.1.20 *Let H and K be finitely generated closed subgroups of a free pro-p group F. Then $H \cap K$ is finitely generated.*

Proof. By Theorem 9.1.19, there exist an open subgroup V of F containing K such that $V = K \amalg M$ (free pro-p product), where M is a closed subgroup of V. Recall that every closed subgroup of F is free pro-p (see Corollary 7.7.5). Hence H is a free pro-p group of finite rank. It follows from Proposition 2.5.5, that $H \cap V$ has finite rank. Let $\{T_i \mid i \in I\}$ be the set of all open subgroups of V containing $H \cap V$. Then, $H \cap V = \bigcap_{i \in I} T_i$. Therefore, $\Phi(H \cap V) = \bigcap_{i \in I} \Phi(T_i)$, by Proposition 2.8.9. By Corollary 9.1.10, $K \cap T_i$ is a free factor of T_i. Hence, by Lemma 9.1.18,

$$\Phi(K \cap T_i) = \Phi(T_i) \cap K \cap T_i = \Phi(T_i) \cap K \ (i \in I).$$

Therefore,

$$\begin{aligned}\Phi(H \cap V) \cap K &= \bigcap_{i \in I}(\Phi(T_i) \cap K) = \bigcap_{i \in I} \Phi(T_i \cap K) \\ &= \Phi(H \cap V \cap K) = \Phi(H \cap K),\end{aligned}$$

where the penultimate equality follows from Proposition 2.8.9. We apply Lemma 9.1.18 again to deduce that $H \cap K = H \cap V \cap K$ is a free factor of $H \cap V$ and therefore is finitely generated. □

Open Question 9.1.21 *Is there a bound on the rank of $H \cap K$ in terms of the ranks of H and K?*

In the abstract case such a bound exists (see Section 9.5).

Exercise 9.1.22 Let $G = G_1 \amalg \cdots \amalg G_n$ be a free pro-p product of pro-p groups and let $g_1, \ldots, g_n$ be elements of G. Prove that

$$G = g_1 G_1 g_1^{-1} \amalg \cdots \amalg g_n G_n g_n^{-1}.$$

We end this section with a proposition, which we only state, generalizing Theorem 8.1.3. A proof can be obtained by mimicking almost word by word the proof of that theorem, and hence, we omit it. [A more general result along these lines can be given for the closed normal closure of S in a free pro-$\mathcal{C}$ product $L = G \amalg S$, where G and S are pro-$\mathcal{C}$ groups; this can be described best using the concept of free pro-$\mathcal{C}$ product of pro-$\mathcal{C}$ groups indexed by a profinite space, which we do not treat in this book.]

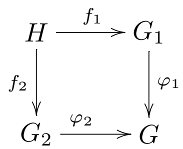
Proposition 9.1.23 *Let $L = G \amalg F$ be the free pro-$\mathcal{C}$ product of a pro-$\mathcal{C}$ group G and a free pro-$\mathcal{C}$ group $F = F_{\mathcal{C}}(X)$ group on a profinite space X. Let N be the smallest closed normal subgroup of L containing F. Then N is the free pro-$\mathcal{C}$ group on the space $R = G \times X$ with canonical map*

$$\iota : R \longrightarrow N$$

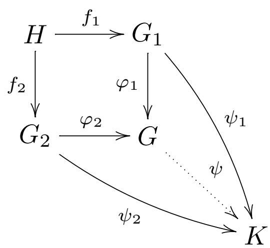
given by $\iota(g, x) = gxg^{-1}$.

9.2 Amalgamated Free Pro-$\mathcal{C}$ Products

Let G_1 and G_2 be pro-$\mathcal{C}$ groups and let $f_i : H \longrightarrow G_i$ $(i = 1, 2)$ be continuous monomorphisms of pro-$\mathcal{C}$ groups. An *amalgamated free pro-$\mathcal{C}$ product* of G_1 and G_2 with amalgamated subgroup H is defined to be a pushout (see Section 2.10)



in the category of pro-$\mathcal{C}$ groups, i.e., a pro-$\mathcal{C}$ group G together with continuous homomorphisms $\varphi_i : G_i \longrightarrow G$ $(i = 1, 2)$ satisfying the following universal property: for any pair of continuous homomorphisms $\psi_1 : G_1 \longrightarrow K$, $\psi_2 : G_2 \longrightarrow K$ into a pro-$\mathcal{C}$ group K with $\psi_1 f_1 = \psi_2 f_2$, there exists a unique continuous homomorphism $\psi : G \longrightarrow K$ such that the following diagram is commutative:



We note that it is enough to check the universal property when $K \in \mathcal{C}$. As a rule, we shall consider H as a common subgroup of G_1 and G_2 and think of f_1 and f_2 as inclusions. An amalgamated free pro-$\mathcal{C}$ product is sometimes referred to as a *free pro-$\mathcal{C}$ product with amalgamation.*

We denote an amalgamated free pro-$\mathcal{C}$ product of G_1 and G_2 with amalgamated subgroup H by $G = G_1 \amalg_H G_2$. This is justified because of the uniqueness of such products as we see in the next proposition.

Proposition 9.2.1 *Let G_1, G_2 and H be pro-$\mathcal{C}$ groups and let $f_i : H \longrightarrow G_i$ $(i = 1, 2)$ be continuous monomorphisms. The free pro-$\mathcal{C}$ product of G_1 and G_2 amalgamating H exists and it is unique.*

Proof. We leave to the reader the task of making precise the meaning of uniqueness and its proof (see the proof of Proposition 9.1.2).

To prove existence we give an explicit construction of

$$G = G_1 \amalg_H G_2.$$

Let $G^{abs} = G_1 *_H G_2$ be the free product of G_1 and G_2 amalgamating H, as abstract groups (see, e.g., Magnus, Karras and Solitar [1966], Lyndon and Schupp [1977] or Serre [1980]). Denote by $\varphi_i^{abs} : G_i \longrightarrow G^{abs}$ the natural embeddings $(i = 1, 2)$. Let

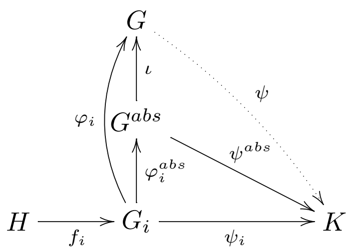
$$\mathcal{N} = \{N \triangleleft_f G^{abs} \mid (\varphi_i^{abs})^{-1}(N) \triangleleft_o G_i \ (i = 1, 2) \text{ and } G^{abs}/N \in \mathcal{C}\}.$$

One easily checks that $\mathcal{N}$ is filtered from below (see Section 3.2). Define $G = \mathcal{K}_{\mathcal{N}}(G^{abs})$ to be the completion of G^{abs} with respect to $\mathcal{N}$. Let $\iota : G^{abs} \longrightarrow G$ be the natural homomorphism. Define $\varphi_i : G_i \longrightarrow G$ by $\varphi_i = \iota\varphi_i^{abs}$ $(i = 1, 2)$. We claim that G together with φ_1 and φ_2 is an amalgamated free pro-$\mathcal{C}$ product of G_1 and G_2 amalgamating H. To see this we check the corresponding universal property.

Let $\psi_i : G_i \longrightarrow K$ $(i = 1, 2)$ be continuous homomorphisms to some $K \in \mathcal{C}$ such that $\psi_1 f_1 = \psi_2 f_2$. Then, by the universal property for abstract amalgamated free products, there exists a unique homomorphism

$$\psi^{abs} : G^{abs} \longrightarrow K$$

with $\psi_i = \psi^{abs}\varphi_i^{abs}$ $(i = 1, 2)$. It follows that $(\varphi_i^{abs})^{-1}(\mathrm{Ker}(\psi^{abs})) = \mathrm{Ker}(\psi_i)$ is open in G_i for every $i = 1, 2$, and since $K \in \mathcal{C}$ one has that $\mathrm{Ker}(\psi^{abs}) \in \mathcal{N}$. Therefore, there exists a continuous homomorphism $\psi : G \longrightarrow K$ with $\psi^{abs} = \psi\iota$. Thus the following diagram



is commutative. This means that $\psi_i = \psi\varphi_i$. The uniqueness of ψ follows from the fact that $G = \overline{\langle\varphi_1(G_1), \varphi_2(G_2)\rangle}$. □

In the abstract situation the canonical homomorphisms

$$\varphi_i^{abs} : G_i \longrightarrow G_1 *_H G_2 \quad (i = 1, 2)$$

are monomorphisms (cf. Theorem I.1 in Serre [1980], for example). Because of this, we usually think of G_i as a subgroup of $G_1 *_H G_2$ $(i = 1, 2)$. In contrast, Examples 9.2.9 and 9.2.10 below show that in the category of pro-$\mathcal{C}$ groups the corresponding maps

$$\varphi_i : G_i \longrightarrow G_1 \amalg_H G_2 \quad (i = 1, 2)$$

are not always injections. An amalgamated free pro-$\mathcal{C}$ product $G = G_1 \amalg_H G_2$ will be called *proper* if the canonical homomorphisms φ_i $(i = 1, 2)$ are monomorphisms. In that case we shall identify G_1, G_2 and H with their images in G, when no possible confusion arises.

The following result is immediate.

Proposition 9.2.2 *Let G_1, G_2 be pro-$\mathcal{C}$ groups and let H be a common closed subgroup of G_1 and G_2. Let $G^{abs} = G_1 *_H G_2$ be an abstract free amalgamated product of pro-$\mathcal{C}$ groups and let*

$$\iota : G^{abs} \longrightarrow \mathcal{K}_{\mathcal{N}}(G^{abs}) = G = G_1 \amalg_H G_2$$

be the canonical homomorphism. Then $G = G_1 \amalg_H G_2$ is proper if and only if $\mathrm{Ker}(\iota) \cap G_i = 1$ *for $i = 1, 2$.*

Remark 9.2.3 If $G = G_1 \amalg_H G_2$ is not proper, one can replace G_1, G_2 and H by their canonical images in G. This operation does not change G, but the amalgamated free pro-$\mathcal{C}$ product $G = G_1 \amalg_H G_2$ becomes proper.

Theorem 9.2.4 *Let $G = G_1 \amalg_H G_2$ be an amalgamated free profinite product of profinite groups. Then the following conditions are equivalent.*

(a) *The natural homomorphism*

$$\iota : G_1 *_H G_2 \longrightarrow G_1 \amalg_H G_2$$

is a monomorphism;

(b) $G = G_1 \amalg_H G_2$ *is proper;*

(c) *There exists an indexing set Λ such that for each $i = 1, 2$, there is a set $\mathcal{U}_i = \{U_{i\lambda} \mid \lambda \in \Lambda\}$ of open normal subgroups of G_i with the following properties*

(1)

$$\bigcap_{\lambda\in\Lambda} U_{i\lambda} = 1 \quad (i = 1, 2); \quad \text{and}$$

(2) *for each* $\lambda \in \Lambda$,

$$U_{1\lambda} \cap H = U_{2\lambda} \cap H.$$

Proof. The implications (a) ⇒ (b) ⇒ (c) are clear.

(c) ⇒ (a): Remark that one may assume that the collections $\mathcal{U}_1$ and $\mathcal{U}_2$ are filtered from below: indeed, if that is not the case, replace $\mathcal{U}_i$ by the collection of all finite intersections of its elements ($i = 1, 2$). It follows from Proposition 2.1.4 that

$$\bigcap_{\lambda\in\Lambda} HU_{1\lambda} = H = \bigcap_{\lambda\in\Lambda} HU_{2\lambda}.$$

Let $1 \neq a \in G_1 *_H G_2$. We have to show that $\iota(a) \neq 1$. Our first aim is to find an appropriate $\lambda \in \Lambda$ (for a purpose that will be explained later). If $a \in H$, choose λ so that $a \notin U_{1\lambda}$. Assume now that $a \notin H$. With no loss of generality, we may assume that a can be written as a finite nonempty product $a = x_1y_1x_2y_2\cdots$, where $x_i \in G_1 - H$ and $y_i \in G_2 - H$, for all i. Then, from our assumptions, there exist some $\lambda \in \Lambda$ such that $x_1, x_2, \ldots \notin HU_{1\lambda}$ and $y_1, y_2, \ldots \notin HU_{2\lambda}$.

In either case, we have $U_{1\lambda} \cap H = U_{2\lambda} \cap H$. Identify $HU_{1\lambda}/U_{1\lambda}$ with $HU_{2\lambda}/U_{2\lambda}$ via the natural isomorphism

$$HU_{1\lambda}/U_{1\lambda} \cong H/(H \cap U_{1\lambda}) = H/(H \cap U_{2\lambda}) \cong HU_{2\lambda}/U_{2\lambda}.$$

Then one has a commutative diagram,

$$\begin{array}{ccc} G_1 *_H G_2 & \xrightarrow{\quad\iota\quad} & G_1 \amalg_H G_2 \\ \downarrow{\scriptstyle\mu} & & \downarrow{\scriptstyle\nu} \\ G_1/U_{1\lambda} *_{HU_{1\lambda}/U_{1\lambda}} G_2/U_{2\lambda} & \xrightarrow{\iota} & G_1/U_{1\lambda} \amalg_{HU_{1\lambda}/U_{1\lambda}} G_2/U_{2\lambda} \end{array}$$

where μ and ν are induced by the canonical epimorphisms $G_i \longrightarrow G_i/U_{i\lambda}$ ($i = 1, 2$). It suffices to prove that $(\nu\iota)(a) \neq 1$. By our choice of $U_{1\lambda}$ and $U_{2\lambda}$, one has that $\mu(a) \neq 1$. Therefore, it suffices to show that

$$\iota : G_1/U_{1\lambda} *_{HU_{1\lambda}/U_{1\lambda}} G_2/U_{2\lambda} \longrightarrow G_1/U_{1\lambda} \amalg_{HU_{1\lambda}/U_{1\lambda}} G_2/U_{2\lambda}$$

is a monomorphism. In other words, we have reduced the problem to the case when the groups G_1 and G_2 are finite. Now, in this case, $G_1 \amalg_H G_2$ is just the profinite completion of $G_1 *_H G_2$ (see the proof of Proposition 9.2.1). Thus, it suffices to show that $G_1 *_H G_2$ is residually finite. This follows from the fact that $G_1 *_H G_2$ contains a normal free subgroup of finite index (see, e.g., Serre [1980], Proposition II.11). □

Exercise 9.2.5 Assume that the equivalent conditions of Theorem 9.2.4 hold. Prove that

$$G_1 \amalg_H G_2 \cong \varprojlim \big(G_1/U_{1\lambda} \amalg_{HU_{1\lambda}/U_{1\lambda}} G_2/U_{2\lambda}\big).$$

Exercise 9.2.6 Let G_1 and G_2 be profinite groups with a common closed subgroup H. Prove that $G_1 \amalg_H G_2$ is proper in each of the following cases:

(a) G_1 and G_2 are isomorphic with the corresponding copies of H identified;
(b) H is in the center of either G_1 or G_2;
(c) H is finitely generated and normal in both G_1 and G_2.

Exercise 9.2.7

(1) Let $G = G_1 *_H G_2$ be an amalgamated free product of abstract groups. Prove that G is residually finite if and only if there exists an indexing set Λ such that for each $i = 1, 2$, there is a set $\mathcal{N}_i = \{N_{i\lambda} \mid \lambda \in \Lambda\}$ of normal subgroups of G_i of finite index with the following properties
   (a) For each $i = 1, 2$, the collection $\mathcal{N}_i = \{N_{i\lambda} \mid \lambda \in \Lambda\}$ is filtered from below;
   (b) $\bigcap_{\lambda\in\Lambda} N_{i\lambda} = 1$, for $i = 1, 2$;
   (c) for each $\lambda \in \Lambda$, $N_{1\lambda} \cap H = N_{2\lambda} \cap H$; and
   (d) $\bigcap_{\lambda\in\Lambda} N_{i\lambda} H = H$ for $i = 1, 2$.
   (Hint: deduce from (a) and (c) that $\tilde{G}_1 = \varprojlim_{\lambda\in\Lambda} G_1/N_{1\lambda}$ and $\tilde{G}_2 = \varprojlim_{\lambda\in\Lambda} G_2/N_{2\lambda}$ have a common subgroup $\tilde{H} = \varprojlim_{\lambda\in\Lambda} H/(H \cap N_{1\lambda})$; then use (b) and (d) to show that the natural homomorphism $G *_H G_2 \longrightarrow \tilde{G}_1 *_{\tilde{H}} \tilde{G}_2$ is injective; and finally show that the sets obtained by taking the closures of $N_{i\lambda}$ in $\tilde{G}_i$ ($\lambda \in \Lambda$, $i = 1, 2$) satisfy the assumptions of Theorem 9.2.4.)
(2) Let $G = G_1 *_H G_2$ be an amalgamated free product of abstract groups. Suppose that G is residually finite and that the profinite topology on G induces the profinite topologies on G_1, G_2 and H. Prove that $\widehat{G} = \widehat{G}_1 \amalg_{\widehat{H}} \widehat{G}_2$ is a proper amalgamated free profinite product of the profinite completions of G_1, G_2 and H.
(3) Let $G = G_1 *_H G_2$ be an amalgamated free product of abstract residually finite groups and suppose H is finite. Prove that G is residually finite and that $\widehat{G} = \widehat{G}_1 \amalg_H \widehat{G}_2$ is a proper amalgamated free profinite product of the profinite completions of G_1 and G_2.

Next we give an example of a nonproper amalgamated free pro-p product. First we need a lemma.

Lemma 9.2.8 *Let A be a finite nontrivial normal subgroup of a pro-p group G. Then A contains a nontrivial element which is in the center of G.*

Proof. This is well-known if G is finite. Let $\varphi : G \longrightarrow \mathrm{Aut}(A)$ the homomorphism that sends an element x of G to the restriction of the inner automorphism determined by x. Let $K = \mathrm{Ker}(\varphi)$. Then G/K is finite. Since the result holds for finite groups, the induced action of G/K on A has a nontrivial fixed point. Since the action of G on A factors through the action of G/K, the result follows. □

Example 9.2.9 Let H be an abelian finitely generated pro-p group of order, say, p^n, where $1 \le n \le \infty$. Put $K = H \times H$. Let T be a procyclic group of order p^n. We shall use additive notation for T and multiplicative notation for H. Define two actions of T on K as follows:

$$t(g,h) = (gh^t, h) \quad \text{and} \quad t(g,h) = (g, g^t h) \quad (t \in T, g, h \in H),$$

(see Section 4.1 for the meaning of h^t and g^t when $T = \mathbf{Z}_p$). We refer to these actions as the 'first' and the 'second' action, respectively. Clearly, these actions are continuous. Define $G_1 = K \rtimes T$ and $G_2 = K \rtimes T$ to be semidirect products using the first and the second action, respectively. Consider the amalgamated free pro-p product $G = G_1 \amalg_K G_2$ of G_1 and G_2 amalgamating K. We show that G is not proper.

Suppose it is proper. Let H_1 be a normal subgroup of index p in H. It is easy to check that $K_1 = H_1 \times H_1$ is normal in G_1 and G_2 and so in G. Then one verifies without difficulty that $G/K_1 = G_1/K_1 \amalg_{K/K_1} G_2/K_1$ (amalgamated free pro-p product), and so it is a proper amalgamated free pro-p product. We claim that $K/K_1 = H/H_1 \times H/H_1$ does not contain nontrivial proper subgroups which are normal in both G_1/K_1 and G_2/K_1. Indeed, assume that Δ is a nontrivial subgroup of K/K_1 which is normal in both G_1/K_1 and G_2/K_1. Let $1 \ne (g,h) \in \Delta$, where $g, h \in H/H_1$. Then either g or h is nontrivial, say $g \ne 1$. Hence, $h = g^t$ for some $1 \le t \le p$. So, using the action of T on $H/H_1 \times H/H_1$ determined by the 'second' action, one has $(-t)(g,h) = (g, g^{-t}h) = (g, 1)$. Now using the action of T on $H/H_1 \times H/H_1$ determined by the 'second' action again, one has $1(g,1) = (g,g)$. Thus we get that $(g,1)$ and $(1,g) = (g^{-1},1)(g,g)$ belong to Δ. Thus $\Delta = K/K_1$. This proves the claim.

It follows that K/K_1 is a finite minimal normal subgroup of G/K_1. However, this is impossible since K/K_1 is noncyclic and contains a central element of G/K_1 according to Lemma 9.2.8. This contradiction proves that G is not proper.

Now we give an example of nonproper free amalgamated product in the category of profinite groups.

Example 9.2.10 Let

$$N_1 = \langle a, b \mid [[a,b],b] = [[a,b],a] = 1\rangle$$

and

$$N_2 = \langle c, d \mid [[c,d],d] = [[c,d],c] = 1\rangle$$

be two copies of a free nilpotent group of class 2 with two generators. Consider the following subgroups $A = \langle a, [a^2, b]\rangle$ and $B = \langle c, [c^2, d]\rangle$ of N_1 and N_2, respectively. Using the identity $[a^2, b] = [a,b]^a[a,b]$, one deduces that a commutes with $[a^2, b]$. Hence the groups A and B are free abelian of rank 2, and so there exist isomorphisms $K = \mathbf{Z} \times \mathbf{Z} \longrightarrow A$ and $K = \mathbf{Z} \times \mathbf{Z} \longrightarrow B$. Let

$N_1 *_K N_2$ be the corresponding free amalgamated product. One knows (see Theorem 1 in Baumslag [1963]) that $N_1 *_K N_2$ is not residually finite. Let $G_1 = \widehat{N}_1$, $G_2 = \widehat{N}_2$ be the profinite completions of N_1 and N_2, respectively. It is easy to see that the closures of A and B in G_1 and G_2, respectively, coincide with their corresponding profinite completions, i.e., $\overline{A} = \widehat{A}$, $\overline{B} = \widehat{B}$. So there are continuous isomorphisms $H \cong \widehat{\mathbf{Z}} \times \widehat{\mathbf{Z}} \longrightarrow \overline{A}$, $H \cong \widehat{\mathbf{Z}} \times \widehat{\mathbf{Z}} \longrightarrow \overline{B}$ induced by the isomorphisms above. Consider the abstract amalgamated free product $G_1 *_H G_2$. Since any finitely generated torsion-free nilpotent group is residually finite (see 5.2.21 in Robinson [1996]), one has natural embeddings $N_1 \longrightarrow G_1$, $N_2 \longrightarrow G_2$. It follows easily that they induce natural embedding $N_1 *_K N_2 \longrightarrow G_1 *_H G_2$. Hence $G_1 *_H G_2$ is not residually finite. Now let $G_1 \amalg_H G_2$ be the amalgamated free profinite product of G_1 and G_2 amalgamating H. We claim that $G_1 \amalg_H G_2$ is not proper. Otherwise, $G_1 *_H G_2$ would be isomorphic to a subgroup of $G_1 \amalg_H G_2$ (see Theorem 9.2.4). This would imply that $G_1 *_H G_2$ is residually finite, a contradiction.

Example 9.2.11 Let X be a proper, nonsingular, connected algebraic curve of genus g over a field $\mathbf{C}$ of complex numbers. As a topological space X is a compact oriented 2-manifold and is simply a sphere with g handles added. The algebraic fundamental group $\pi_1(X)$ in the sense of SGA-1 [1971] is the profinite completion of the fundamental group $\pi_1^{top}(X)$ in the topological sense (see Exp. 10, page 272 in SGA-1 [1971]). The (abstract) group $\pi_1^{top}(X)$ is called a surface group and has $2g$ generators a_i, b_i $(i = 1, \ldots, g)$ subject to one relation $[a_1, b_1][a_2, b_2] \cdots [a_g, b_g] = 1$. It follows that the profinite group $\pi_1(X)$ has exactly the same presentation. It is easy to see then that

$$\pi_1(X) = \overline{\langle a_1, b_1\rangle} \amalg_{[b_1,a_1]=[a_2,b_2]\cdots[a_g,b_g]} \overline{\langle a_2, b_2, \ldots, a_g, b_g\rangle} \cong F_2 \amalg_{\widehat{\mathbf{Z}}} F_{2g-2}$$

is a profinite proper free amalgamated product of free profinite groups of ranks 2 and $2g-2$ with a procyclic amalgamated subgroup for $g > 1$.

Example 9.2.12 A Demushkin group is a pro-p group G having one of the following presentation (see Labute [1967], Theorem 1):

(a)
$$G = \langle a_1, b_1, \ldots, a_g, b_g \mid a_1^{p^n}[a_1, b_1] \cdots [a_g, b_g]\rangle,$$

where $p > 2$ and n is a natural number or ∞ (the latter just means that $a_1^{p^n} = 1$);

(b)
$$G = \langle a_1, b_1, \ldots, a_g, b_g \mid a_1^{2+2^n}[a_1, b_1] \cdots [a_g, b_g]\rangle,$$

where $p = 2$ and $n > 1$ or ∞;

(c)
$$G = \langle a_1, b_1, \ldots, a_g, b_g \mid a_1^2[a_1, b_1]a_2^{2n}[a_2, b_2] \cdots [a_g, b_g]\rangle,$$

where $p = 2$ and $n > 1$.

If $g > 1$ then a Demushkin group splits as a proper free pro-p product with procyclic amalgamation in one of the following form:

(a)
$$\overline{\langle a_1, b_1\rangle} \amalg_{[b_1,a_1]a_1^{-p^n}=[a_2,b_2]\cdots[a_g,b_g]} \overline{\langle a_2, b_2, \dots, a_g, b_g\rangle};$$

(b)
$$\overline{\langle a_1, b_1\rangle} \amalg_{[b_1,a_1]a_1^{-2-2^n}=[a_2,b_2]\cdots[a_g,b_g]} \overline{\langle a_2, b_2, \dots, a_g, b_g\rangle};$$

(c)
$$\overline{\langle a_1, b_1\rangle} \amalg_{[b_1,a_1]a_1^{-2}=a_2^{2^n}[a_2,b_2]\cdots[a_g,b_g]} \overline{\langle a_2, b_2, \dots, a_g, b_g\rangle}.$$

Note that if $p > 2$ and $n = \infty$ then a Demushkin group is a maximal pro-p quotient of the algebraic fundamental group of an algebraic curve of genus g from the preceding example.

There are Mayer-Vietoris sequences associated with an amalgamated free pro-$\mathcal{C}$ product. We state them in the following theorem without proof (cf. Gildenhuys and Ribes [1974], Theorem 1.13).

Proposition 9.2.13 *Let $\mathcal{C}$ be an extension closed variety of finite groups. Let $G = G_1 \amalg_H G_2$ be a proper amalgamated free pro-$\mathcal{C}$ product of pro-$\mathcal{C}$ groups. Then*

(a) *for any left discrete $[\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]$-module A, there is a long exact sequence*

$$\begin{aligned} 1 &\to H^0(G,A) \xrightarrow{\text{Res}} H^0(G_1,A) \oplus H^0(G_2,A) \to H^0(H,A) \\ &\to \cdots \to H^n(G,A) \xrightarrow{\text{Res}} H^n(G_1,A) \oplus H^n(G_2,A) \to H^n(H,A) \\ &\to H^{n+1}(G,A) \to \cdots \end{aligned}$$

where Res *is induced by the restrictions* $\text{Res}^G_{G_i} : H^n(G,A) \longrightarrow H^n(G_i,A)$ $(i = 1, 2)$;

(b) *for any profinite right $[\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]$-module B, there is a long exact sequence*

$$\begin{aligned} \cdots &\to H_{n+1}(G,B) \to H_n(H,B) \to H_n(G_1,B) \oplus H_n(G_2,B) \\ &\xrightarrow{\text{Cor}} H_n(G,B) \to \cdots \to H_1(G,B) \to H_0(H,B) \\ &\to H_0(G_1,B) \oplus H_0(G_2,B) \xrightarrow{\text{Cor}} H_0(G,B) \to 1, \end{aligned}$$

where Cor *is induced by corestrictions* $\text{Cor}^G_{G_i} : H_n(G_i,B) \longrightarrow H_n(G,B)$, $i = 1, 2$.

9.3 Cohomological Characterizations of Amalgamated Products

Let H be a pro-$\mathcal{C}$ group and let L be a closed subgroup of H. For $A \in$ $\mathbf{DMod}([\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!])$, define

$$\mathrm{Der}_L(H,A) = \{d : H \longrightarrow A \mid d(xy) = xd(y) + d(x),\ \forall x, y \in H,\ d_{|L} = 0\},$$

the abelian group of all continuous derivations from H to A vanishing on L.

Our aim is to prove the following criterion to decide, in terms of derivations, when a pro-$\mathcal{C}$ group H is a free pro-$\mathcal{C}$ product of two of its subgroups amalgamating a common subgroup.

Theorem 9.3.1 *Let $\mathcal{C}$ be an extension closed variety of finite solvable groups. Let H_1 and H_2 be closed subgroups of a pro-$\mathcal{C}$ group H. Assume that $L \leq_c H_1 \cap H_2$. Then*

$$H = H_1 \amalg_L H_2$$

(*amalgamated free pro-$\mathcal{C}$ product*) *if and only if the natural homomorphism*

$$\varPhi_H : \mathrm{Der}_L(H,A) \longrightarrow \mathrm{Der}_L(H_1,A) \times \mathrm{Der}_L(H_2,A)$$

($f \mapsto (f_{|H_1}, f_{|H_2})$, $f \in \mathrm{Der}_L(H,A)$) *is an isomorphism for all $[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]$-modules $A \in \mathcal{C}$.*

Before proving this theorem we need some auxiliary results. Remark that under the conditions of the theorem above, the amalgamated free pro-$\mathcal{C}$ product $H = H_1 \amalg_L H_2$ is always proper, as one easily sees using the criterion given in Theorem 9.2.4, for example (one can also see this directly by using the universal property of an amalgamated product).

Clearly $\mathrm{Der}_L(H,-)$ is a left exact additive functor from the category $\mathbf{DMod}([\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!])$ to the category $\mathfrak{A}$ of abelian groups.

Consider the continuous monomorphism of $[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]$-modules

$$\nu : A \longrightarrow \mathrm{Coind}_L^H(A)$$

given by $\nu(a)(x) = xa$ ($a \in A, x \in H$). One can identify $\nu(A)$ with the following submodule of $\mathrm{Coind}_L^H(A)$

$$\nu(A) = \{f : H \longrightarrow A \mid f(xy) = xf(y),\ \forall x, y \in H\}.$$

Define

$$\varGamma(A) = \mathrm{Coind}_L^H(A)/\nu(A).$$

Then we have a short exact sequence

$$0 \longrightarrow A \stackrel{\nu}{\longrightarrow} \mathrm{Coind}_L^H(A) \longrightarrow \varGamma(A) \longrightarrow 0. \qquad (3)$$

Lemma 9.3.2

$$\varGamma(-) : \mathbf{DMod}([\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]) \longrightarrow \mathfrak{A}$$

is an exact functor.

Proof. This is a consequence of Proposition 6.10.4. □

Lemma 9.3.3 *Let $L \leq_c H$ be pro-$\mathcal{C}$ groups. For each $A \in \mathbf{DMod}([\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!])$, there is a natural isomorphism*

$$\varphi_A : \mathrm{Hom}_{[\![\widehat{\mathbf{Z}}_{\mathcal{C}} H]\!]}(\widehat{\mathbf{Z}}_{\mathcal{C}}, \Gamma(A)) \cong \mathrm{Der}_L(H, A).$$

Proof. Clearly $\mathrm{Hom}_{[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A)) = \Gamma(A)^H$. Let $f \in \mathrm{Coind}_L^H(A)$ be such that $f + \nu(A) \in \Gamma(A)^H$. Then $zf - f \in \nu(A)$ for each $z \in H$. So, for all $x, y, z \in H$, one has

$$(zf - f)(xy) = x[(zf - f)(y)] = xf(yz) - xf(y),$$

and on the other hand,

$$(zf - f)(xy) = f(xyz) - f(xy).$$

Letting $z = y^{-1}$, we deduce that

$$f(xy) = xf(y) + f(x) - xf(1), \ \forall x, y \in H.$$

Define $f_c \in \nu(A)$ to be the map $x \mapsto xf(1)$ $(x \in H)$. Hence, $f - f_c \in \mathrm{Der}_L(H, A)$. Define $\varphi_A(f + \nu(A)) = f - f_c$. Clearly φ_A is a natural monomorphism. To prove that φ_A is an epimorphism, let $d \in \mathrm{Der}_L(H, A)$. Then $d \in \mathrm{Coind}_L^H(A)$. Claim that $d + \nu(A) \in \Gamma(A)^H$. To see this we must show that if $z \in H$, then $zd - d \in \nu(A)$. Indeed,

$$(zd - d)(x) = d(xz) - d(z) = xd(z), \quad \forall x \in H,$$

i.e., $zd - d$ is the function $x \mapsto xd(z)$, which belongs to $\nu(A)$. Finally, observe that $d(1) = 0$; thus $\varphi_A(d + \nu(A)) = d$. □

Corollary 9.3.4 *Let H be a pro-$\mathcal{C}$ group and assume $L \leq_c H$. Then*

$$\{\mathrm{Ext}^n_{[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(-))\}_{n \geq 0}$$

is the sequence of right derived functors of the left exact functor $\mathrm{Der}_L(H, -)$ in the category $\mathbf{DMod}([\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!])$.

Proof. Observe that the sequence of functors

$$\{\mathrm{Ext}^n_{[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(-))\}_{n \geq 0}$$

is a cohomological sequence since $\Gamma(-)$ is an exact functor by Lemma 9.3.2. We claim that this sequence is effaceable, i.e., $\mathrm{Ext}^n_{[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A)) = 0$ whenever A is injective and $n \geq 1$. This follows from Corollary 6.10.3 by considering the long exact sequence

$$\cdots \longrightarrow \mathrm{Ext}^n_H(\mathbf{Z}_{\hat{\mathcal{C}}}, A) \longrightarrow \mathrm{Ext}^n_H(\mathbf{Z}_{\hat{\mathcal{C}}}, \mathrm{Coind}_L^H(A)) \longrightarrow \mathrm{Ext}^n_H(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A)) \longrightarrow \cdots$$

obtained by applying $\{\mathrm{Ext}^n_{[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, -)\}_{n \geq 0}$ to (3) (here $\mathrm{Ext}^n_H(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A))$ stands for $\mathrm{Ext}^n_{[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A))$). The result follows now from Lemma 9.3.3 and Lemma 6.1.4. □

Proposition 9.3.5 *Let H be a pro-$\mathcal{C}$ group and assume $L \leq_c H$. Let $A \in$ $\mathbf{DMod}([\![\mathbf{Z}_{\hat{\mathcal{C}}}H]\!])$. Then*

(a) *There exists an exact sequence*

$$\begin{aligned} 0 \longrightarrow A^H \longrightarrow A^L \longrightarrow \operatorname{Ext}^0_{[\![\mathbf{Z}_{\hat{\mathcal{C}}}H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, \varGamma(A)) \longrightarrow H^1(H,A) \\ \longrightarrow H^1(L,A) \longrightarrow \operatorname{Ext}^1_{[\![\mathbf{Z}_{\hat{\mathcal{C}}}H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, \varGamma(A)) \longrightarrow H^2(H,A) \longrightarrow \cdots; \end{aligned}$$

(b) *If*

$$\begin{array}{ccc} H' & \xrightarrow{\ \rho\ } & H \\ \uparrow & & \uparrow \\ L' & \xrightarrow{\ \rho_{|L'}\ } & L \end{array}$$

is a commutative diagram of pro-$\mathcal{C}$ groups and continuous homomorphisms, then there is a corresponding commutative diagram

$$\begin{array}{ccccccc} \cdots \longrightarrow & \operatorname{Ext}^0_{[\![\mathbf{Z}_{\hat{\mathcal{C}}}H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, \varGamma(A)) & \longrightarrow & H^1(H,A) & \longrightarrow & H^1(L,A) & \longrightarrow \cdots \\ & \downarrow & & \downarrow & & \downarrow & \\ \cdots \longrightarrow & \operatorname{Ext}^0_{[\![\mathbf{Z}_{\hat{\mathcal{C}}}H']\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, \varGamma(A)) & \longrightarrow & H^1(H',A) & \longrightarrow & H^1(L',A) & \longrightarrow \cdots \end{array}$$

where the vertical maps are induced by ρ.

Proof. (a) It follows from the definition of group cohomology that

$$\operatorname{Ext}^n_{[\![\mathbf{Z}_{\hat{\mathcal{C}}}H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, A) = H^n(H,A).$$

By Theorem 6.10.5,

$$\operatorname{Ext}^n_{[\![\mathbf{Z}_{\hat{\mathcal{C}}}H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, \operatorname{Coind}^H_L(A)) = H^n(L,A).$$

Hence the exact sequence of part (a) is just the long exact sequence obtained by applying the cohomological functor $\{\operatorname{Ext}^n_{[\![\mathbf{Z}_{\hat{\mathcal{C}}}H]\!]}(\mathbf{Z}_{\hat{\mathcal{C}}}, -)\}_{n\geq 0}$ to the short exact sequence (3).

Part (b) is left as an exercise. □

Lemma 9.3.6 *Assume that the variety $\mathcal{C}$ is extension closed. Let G be a profinite group and let A be a finite discrete G-module. Denote by*

$$\tilde{G} = A \rtimes G$$

the corresponding semidirect product. Let $d : G \longrightarrow A$ be a continuous derivation. Then the map $\rho : G \longrightarrow \tilde{G}$, given by $x \mapsto (d(x), x)$ $(x \in G)$, is a continuous homomorphism of profinite groups. Conversely, if $\rho : G \longrightarrow \tilde{G}$ is a continuous homomorphism such that $\rho(x) = (d(x), x)$ $(x \in G)$, where $d : G \longrightarrow A$ is a function, then d is a continuous derivation.

Proof. This follows from the definition of multiplication in $\tilde{G} = A \rtimes G$:

$$(a,x)(a',x') = (a + xa', xx') \quad (a, a' \in A, x, x' \in G). \qquad \square$$

Lemma 9.3.7 *Let H_1 and H_2 be closed subgroups of a pro-$\mathcal{C}$ group H and let $L \leq_c H_1 \cap H_2$. Assume that the natural homomorphism*

$$\Phi_H : \mathrm{Der}_L(H, A) \longrightarrow \mathrm{Der}_L(H_1, A) \times \mathrm{Der}_L(H_2, A)$$

($f \mapsto (f_{|H_1}, f_{|H_2})$, $f \in \mathrm{Der}_L(H, A)$), is a monomorphism for all simple $[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]$-modules $A \in \mathcal{C}$. Then the closed subgroup of H generated by H_1 and H_2 is H.

Proof. For a closed subgroup T of H, denote by $\omega(T)$ the closed left ideal of $[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]$ generated by the subspace $\{t - 1 \mid t \in T\}$. Then the map ω in an injection. One sees this by observing that the natural module homomorphism $[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!] \longrightarrow [\![\mathbf{Z}_{\hat{\mathcal{C}}}(H/T)]\!]$ sends $\omega(T)$ to the zero submodule.

Let S be the closed subgroup of H generated by H_1 and H_2. Assume that $H > S$. Define

$$\omega(H, S) = \omega(H)/\omega(S).$$

Then $\omega(H, S)$ is a nonzero profinite $[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]$-module. Let $\omega(H, S) \longrightarrow A$ be an epimorphism onto a finite discrete simple $[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]$-module (see Lemma 5.1.1). Define

$$d : H \longrightarrow \omega(H, S)$$

by $d(x) = (x - 1) + \omega(S)$ $(x \in H)$. One readily checks that

$$d \in \mathrm{Der}_L(H, \omega(H, S)).$$

Denote the composition

$$H \xrightarrow{d} \omega(H, S) \longrightarrow A$$

by f. Then $f \in \mathrm{Der}_L(H, A)$ and $f \neq 0$. However, $\Phi_H(f) = 0$, a contradiction. Thus $S = H$, as desired. $\square$

Proposition 9.3.8 *Let $\mathcal{C}$ be an extension closed variety of finite groups. Assume that $H = H_1 \amalg_L H_2$ is a free pro-$\mathcal{C}$ product of two pro-$\mathcal{C}$ groups H_1 and H_2 amalgamating a common closed subgroup L. Then, for every pro-$\mathcal{C}$ $[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]$-module A, the natural homomorphism*

$$\Phi_H : \mathrm{Der}_L(H, A) \longrightarrow \mathrm{Der}_L(H_1, A) \times \mathrm{Der}_L(H_2, A)$$

($f \mapsto (f_{|H_1}, f_{|H_2})$, $f \in \mathrm{Der}_L(H, A)$), is an isomorphism.

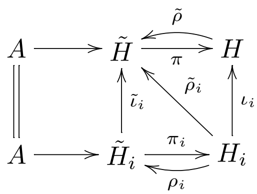
Proof. Express $A = \varinjlim A_i$, where each $A_i \in \mathcal{C}$ is a finite $[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]$-module. Since $\mathrm{Der}_L(H, -)$ commutes with direct limits (this can be seen by an argument similar to the one used in Lemma 5.1.4), one may assume that $A \in \mathcal{C}$. We shall exhibit an inverse homomorphism

$$\Psi : \mathrm{Der}_L(H_1, A) \times \mathrm{Der}_L(H_2, A) \longrightarrow \mathrm{Der}_L(H, A)$$

of Φ_H. Let $d_i \in \mathrm{Der}_L(H_i, A)$ $(i = 1, 2)$. Since $A \in \mathcal{C}$, the semidirect products $\tilde{H}_i = A \rtimes H_i$ $(i = 1, 2)$ are pro-$\mathcal{C}$ groups. For $i = 1, 2$, define

$$\rho_i : H_i \longrightarrow \tilde{H}_i = A \rtimes H_i$$

by $\rho_i(x) = (d_i(x), x)$ $(x \in H_i)$. By Lemma 9.3.6, ρ_i is a continuous homomorphism. Consider the following commutative diagram for each $i = 1, 2$:



where π and π_i are the canonical projections, and ι_i and $\tilde{\iota}_i$ are the inclusion maps $(i = 1, 2)$. Put $\tilde{\rho}_i = \tilde{\iota}_i \rho_i$ $(i = 1, 2)$. Plainly, $\tilde{\rho}_1$ and $\tilde{\rho}_2$ coincide on L. Hence they induce a continuous homomorphism $\tilde{\rho} : H \longrightarrow \tilde{H} = A \rtimes H$, by the universal property of amalgamated products. Since $\pi\tilde{\rho}_i(x) = x$ for all $x \in H_i$ $(i = 1, 2)$, it follows that $\pi\tilde{\rho}(x) = x$ for all $x \in H$. Therefore, $\tilde{\rho}(x) = (d(x), x)$, where $d : H \longrightarrow A$ is a derivation (see Lemma 9.3.6). Define $\Psi(d_1, d_2) = d$. One easily checks that Φ_H and Ψ are inverse to each other. □

Proof of Theorem 9.3.1. In one direction this follows from Proposition 9.3.8. Conversely, assume that Φ_H is an isomorphism. Consider the amalgamated free pro-$\mathcal{C}$ product $G = H_1 \amalg_L H_2$, and denote by $\varphi : G \longrightarrow H$ the continuous homomorphism induced by the inclusions $H_i \hookrightarrow H$ $(i = 1, 2)$. By Lemma 9.3.7, $H = \overline{\langle H_1, H_2 \rangle}$; hence φ is an epimorphism. To show that φ is an isomorphism, it suffices to prove that the conditions of Proposition 7.2.7 are satisfied, i.e., that for every (simple) H-module A, the map φ induces an epimorphism $\varphi^1 : H^1(H, A) \longrightarrow H^1(G, A)$ and a monomorphism $\varphi^2 : H^2(H, A) \longrightarrow H^2(G, A)$. We shall show in fact that φ^1 and φ^2 are isomorphisms. Consider the infinite commutative diagram

$$\begin{array}{ccccccccccc}
A^L & \longrightarrow & \mathrm{Ext}^0_H & \longrightarrow & H^1(H, A) & \longrightarrow & H^1(L, A) & \longrightarrow & \mathrm{Ext}^1_H & \longrightarrow & H^2(H, A) \\
\| & & \downarrow{\scriptstyle \bar{\varphi}^0} & & \downarrow{\scriptstyle \varphi^1} & & \| & & \downarrow{\scriptstyle \bar{\varphi}^1} & & \downarrow{\scriptstyle \varphi^2} \\
A^L & \longrightarrow & \mathrm{Ext}^0_G & \longrightarrow & H^1(G, A) & \longrightarrow & H^1(L, A) & \longrightarrow & \mathrm{Ext}^1_G & \longrightarrow & H^2(G, A)
\end{array}$$

with exact rows and vertical maps induced by φ (see Proposition 9.3.5), where Ext^n_H stands for $\mathrm{Ext}^n_H(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A))$ and Ext^n_G for $\mathrm{Ext}^n_G(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A))$.

By our assumptions and by the first part of the proof, we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Der}_L(H,A) & & \\ & \searrow^{\Phi_H} & \\ \bar{\varphi}\downarrow & & \mathrm{Der}_L(H_1,A) \times \mathrm{Der}_L(H_2,A) \\ & \nearrow_{\Phi_G} & \\ \mathrm{Der}_L(G,A) & & \end{array}$$

where $\bar{\varphi}$ is induced by φ and Φ_H and Φ_G are isomorphisms. Therefore $\bar{\varphi}$ is an isomorphism. It follows from Corollary 9.3.4 that the maps

$$\bar{\varphi}^n : \mathrm{Ext}^n_H(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A)) \longrightarrow \mathrm{Ext}^n_G(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A))$$

are isomorphisms for $n \geq 0$ (note that it is here where one needs that the isomorphism Φ_H is valid for all $[\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!]$-modules $A \in \mathcal{C}$, not just for simple modules). Thus one infers from the 'Five Lemma' (cf. Mac Lane [1963], Lemma I.3.3) and the above infinite diagram that $\varphi^n : H^n(H,A) \longrightarrow H^n(G,A)$ are isomorphisms, as desired. □

Proposition 9.3.9 *Let $\mathcal{C}$ be an extension closed variety of finite groups. Assume that $H = H_1 \amalg H_2$ is a free pro-$\mathcal{C}$ product of two pro-$\mathcal{C}$ groups H_1 and H_2. Then, for every $A \in \mathbf{DMod}([\![\mathbf{Z}_{\hat{\mathcal{C}}} H]\!])$ we have that*

(a)

$$\Phi_H : \mathrm{Der}(H,A) \xrightarrow{\cong} \mathrm{Der}(H_1,A) \times \mathrm{Der}(H_2,A)$$

is an isomorphism, where the homomorphism Φ_H is given by $f \mapsto (f_{|H_1}, f_{|H_2})$ ($f \in \mathrm{Der}_L(H,A)$), and

(b)

$$\Phi^n_H : H^n(H,A) \xrightarrow{\cong} H^n(H_1,A) \times H^n(H_2,A) \quad (n \geq 2)$$

are isomorphisms, where the homomorphisms Φ^n_H are induced by the restriction maps.

Proof. Part (a) is a special case of Proposition 9.3.8. For part (b), assume first that $L = 1$ and consider the exact sequence (3). It follows from the long exact sequence of Proposition 9.3.5(a) that, if $L = 1$, then

$$\mathrm{Ext}^n_H(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A)) = H^{n+1}(H,A) \quad \forall n \geq 1$$

and

$$\mathrm{Ext}^0_H(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(A)) = \mathrm{Der}(H,A).$$

Since every injective $\mathbf{DMod}([\![\mathbf{Z}_{\hat{\mathcal{C}}}H]\!]$-module is $\mathbf{DMod}([\![\mathbf{Z}_{\hat{\mathcal{C}}}H_i]\!]$-injective ($i = 1.2$) (see Corollary 5.7.2), it follows that the cohomological functors

$$\{\mathrm{Ext}^n_H(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(-))\}_{n\geq 0} \quad \text{and} \quad \{\mathrm{Ext}^n_{H_2}(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(-)) \times \mathrm{Ext}^n_{H_1}(\mathbf{Z}_{\hat{\mathcal{C}}}, \Gamma(-))\}_{n\geq 0}$$

are universal. The result follows then from Part (a). □

Theorem 9.3.10 *Let p be a prime number. Let H_1 and H_2 be closed subgroups of a pro-p group H. Then,*

$$H = H_1 \amalg H_2$$

(*the free pro-p product*) *if and only if*

(a)
$$\Phi^1_H : H^1(H, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^1(H_1, \mathbf{Z}/p\mathbf{Z}) \times H^1(H_2, \mathbf{Z}/p\mathbf{Z})$$
is an epimorphism,

(b)
$$\Phi^2_H : H^2(H, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^2(H_1, \mathbf{Z}/p\mathbf{Z}) \times H^2(H_2, \mathbf{Z}/p\mathbf{Z})$$
is a monomorphism (*here Φ^n_H is induced by the restriction maps* ($n = 1, 2$)).

Proof. In one direction, this follows from Proposition 9.3.9. Conversely, assume that (a) and (b) hold. Since $\mathbf{Z}/p\mathbf{Z}$ is a trivial H-module, we have

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

for $G = H$, H_1 or H_2. Hence by Lemma 9.3.7, H is generated by H_1 and H_2 (as a pro-p group). Set $G = H_1 \amalg H_2$ (the free pro-p product). Let

$$\varphi : G \longrightarrow H$$

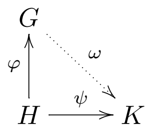
the homomorphism induced by the inclusions $H_i \hookrightarrow H$ ($i = 1, 2$). Then φ is an epimorphism. Consider the commutative diagram

$$\begin{array}{ccc} H^n(H, \mathbf{Z}/p\mathbf{Z}) & & \\ & \searrow^{\Phi^n_H} & \\ \downarrow{\scriptstyle \bar{\varphi}^n} & & H^n(H_1, \mathbf{Z}/p\mathbf{Z}) \times H^n(H_2, \mathbf{Z}/p\mathbf{Z}) \\ & \nearrow_{\Phi^n_G} & \\ H^n(G, \mathbf{Z}/p\mathbf{Z}), & & \end{array}$$

where $\bar{\varphi}^n$ is induced by φ and Φ^n_G is induced by Φ_G as defined in Proposition 9.3.9. Since Φ^n_G is an isomorphism for every n, it follows from our assumptions that $\bar{\varphi}^1$ is an epimorphism and $\bar{\varphi}^2$ a monomorphism. Therefore φ is an isomorphism by Proposition 7.2.7. □

9.4 Pro-$\mathcal{C}$ HNN-extensions

Let H be a pro-$\mathcal{C}$ group and let $f : A \longrightarrow B$ be a continuous isomorphism between closed subgroups A, B of H. A *pro-$\mathcal{C}$ HNN-extension* of H with associated subgroups A, B consists of a pro-$\mathcal{C}$ group $G = \mathrm{HNN}(H, A, f)$, an element $t \in G$, and a continuous homomorphism $\varphi : H \longrightarrow G$ with $t(\varphi(a))t^{-1} = \varphi f(a)$ and satisfying the following universal property: for any pro-$\mathcal{C}$ group K, any $k \in K$ and any continuous homomorphism $\psi : H \longrightarrow K$ satisfying $k(\psi(a))k^{-1} = \psi f(a)$ for all $a \in A$, there is a unique continuous homomorphism $\omega : G \longrightarrow K$ with $\omega(t) = k$ such that the diagram



is commutative. We shall refer to ω as the homomorphism induced by ψ.

Observe that one needs to test the above universal property only for finite groups $K \in \mathcal{C}$, for then it holds automatically for any pro-$\mathcal{C}$ group K, since K is an inverse limit of groups in $\mathcal{C}$.

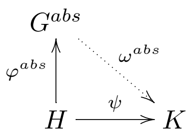
Proposition 9.4.1 *Let H be a pro-$\mathcal{C}$ group and let $f : A \longrightarrow B$ be an isomorphism of subgroups of H. Then there exists a unique pro-$\mathcal{C}$ HNN-extension $G = \mathrm{HNN}(H, A, f)$.*

Proof. The uniqueness follows easily from the universal property. We give an explicit construction of $G = \mathrm{HNN}(H, A, f)$ to prove the existence. Let $G^{abs} = \mathrm{HNN}^{abs}(H, A, f)$ be the abstract HNN-extension. Denote by $\varphi^{abs} : H \longrightarrow G^{abs}$ the natural embedding. Let

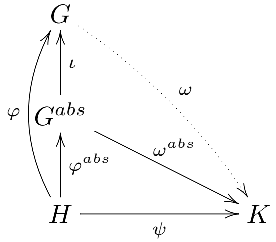
$$\mathcal{N} = \{N \triangleleft_f G^{abs} \mid (\varphi^{abs})^{-1}(N) \triangleleft_o H, G/N \in \mathcal{C}\}.$$

Define $G = \mathcal{K}_{\mathcal{N}}(G^{abs})$ to be the completion of G^{abs} with respect to $\mathcal{N}$. Let $\iota : G^{abs} \longrightarrow G$ be the natural homomorphism. Put $\varphi = \iota\varphi^{abs}$. We check the universal property for G and φ.

Let $\psi : H \longrightarrow K$ be a continuous homomorphism to some $K \in \mathcal{C}$ with $k(\psi(a))k^{-1} = \psi f(a)$ for all $a \in A$. Then, by the universal property for abstract HNN-extensions, there is a unique homomorphism $\omega^{abs} : G^{abs} \longrightarrow K$ with $\omega^{abs}(t) = k$ such that the diagram



is commutative. It follows that $(\varphi^{abs})^{-1}(\mathrm{Ker}(\omega^{abs})) = \mathrm{Ker}(\psi)$ is open in H, and since $K \in \mathcal{C}$, one has that $\mathrm{Ker}(\omega^{abs}) \in \mathcal{N}$. Therefore, there exists a continuous homomorphism $\omega : G \longrightarrow K$ with $\omega^{abs} = \omega\iota$. Thus the following diagram



is commutative. This means that $\psi = \omega\varphi$ and $\omega(t) = k$. The uniqueness of ω follows from the fact that $G = \overline{\langle \varphi(H), \iota(t)\rangle}$. □

In contrast with the abstract situation, the canonical homomorphism $\varphi : H \longrightarrow G = \mathrm{HNN}(H, A, f)$ is not always a monomorphism. When φ is a monomorphism, we shall call $G = \mathrm{HNN}(H, A, f)$ a *proper* pro-$\mathcal{C}$ HNN-extension.

Associated with a pro-$\mathcal{C}$ HNN-extension, there exist Mayer-Vietoris sequences analogous to those obtained for abstract groups. We present them in the following theorem without proof.

Proposition 9.4.2 *Let $\mathcal{C}$ be an extension closed variety of finite groups. Let $G = \mathrm{HNN}(H, A, f)$ be a proper pro-$\mathcal{C}$ HNN-extension of pro-$\mathcal{C}$ groups and $\pi = \pi(\mathcal{C})$. Then*

(a) *for any left discrete $\mathbf{Z}_{\hat{\mathcal{C}}}[\![G]\!]$-module M there is a long exact sequence*

$$\begin{aligned} 1 \to H^0(G, M) \xrightarrow{\mathrm{Res}} H^0(H, M) \to H^0(A, M) \to H^1(G, M) \to \cdots \\ \to H^n(G, M) \to H^n(H, M) \to H^n(A, M) \to H^{n+1}(G, M) \to \cdots, \end{aligned}$$

where Res *is the restriction* $\mathrm{Res}^G_H : H^n(G, M) \longrightarrow H^n(H, M)$;

(b) *for any profinite right $\mathbf{Z}_{\hat{\pi}}[\![G]\!]$-module M there is a long exact sequence*

$$\begin{aligned} \cdots \to H_{n+1}(G, M) \to H_n(A, M) \to H_n(H, M) \overset{\mathrm{Cor}}{\to} H_n(G, M) \to \cdots \\ \to H_1(G, M) \to H_0(A, M) \to H_0(H, M) \overset{\mathrm{Cor}}{\to} H_0(G, M) \to 1, \end{aligned}$$

where Cor *is the corestriction* $\mathrm{Cor}^G_H : H_n(H, M) \longrightarrow H_n(G, M)$*, $i = 1, 2$.*

From now on in this section we assume that $\mathcal{C}$ is the variety of all finite groups.

The next proposition gives a sufficient condition for a profinite HNN-extension to be proper.

Proposition 9.4.3 *Let $G = \mathrm{HNN}(H, A, f)$ be a profinite HNN-extension of profinite groups and let $\varphi : H \longrightarrow G$ be the canonical homomorphism. Then*

(1) $\mathrm{Ker}(\varphi) = K$, *where*

$$K = \left\{ \bigcap U \mid U \triangleleft_o H, f(A \cap U) = f(A) \cap U \right\}.$$

(2) $G = \mathrm{HNN}(H, A, f)$ *is proper if and only if for every open normal subgroup* U *of* H *there is an open normal subgroup* V *of* H *contained in* U *and such that*

$$f(A \cap V) = f(A) \cap V$$

(*or equivalently, if and only if* K *is trivial*). *In particular, if* A *is finite, then* G *is proper.*

(3) $G = \mathrm{HNN}(H, A, f)$ *is a proper profinite HNN-extension if and only if* $\mathrm{HNN}^{abs}(H, A, f)$ *embeds in* G *and therefore is residually finite.*

Proof. (1) Let $G^{abs} = \mathrm{HNN}^{abs}(H, A, f)$ be the abstract HNN-extension. We identify H with its natural image in G^{abs}. Let $\mathcal{N} = \{N \triangleleft_f G \mid N \cap H \leq_o H\}$. From the explicit construction of $G = \mathrm{HNN}(H, A, f)$ (see the proof of Proposition 9.4.1), it follows that

$$\mathrm{Ker}(\varphi) = \bigcap_{N \in \mathcal{N}} (N \cap H).$$

Since $N \cap H$ is an open normal subgroup of H for any $N \in \mathcal{N}$, we deduce from $f(A \cap N) = (A \cap N)^t = A^t \cap N = f(A) \cap N$, that $K \leq \mathrm{Ker}(\varphi)$.

Conversely, let U be an open normal subgroup of H such that $f(A \cap U) = f(A) \cap U$. The isomorphisms $A/(A \cap U) \cong AU/U$ and $f(A)/(f(A) \cap U) \cong f(A)U/U$ induce an isomorphism $f_U : AU/U \longrightarrow f(A)U/U$. Let $G_U = \mathrm{HNN}(H/U, AU/U, f_U)$ be the profinite HNN-extension of H/U with associated subgroups AU/U and $f_U(AU/U)$. By the universal property, there exists a continuous homomorphism $\omega_U : G \longrightarrow G_U$ induced by the natural epimorphism $\psi_U : H \longrightarrow H_U$. Hence one has the following commutative diagram:

$$\begin{array}{ccc} G & \xrightarrow{\omega_U} & G_U \\ {\scriptstyle\varphi}\uparrow & & \uparrow{\scriptstyle\varphi_U} \\ H & \xrightarrow{\psi_U} & H_U \end{array}$$

where φ_U is the canonical homomorphism. Since H_U is finite, it follows from the explicit construction of a profinite HNN-extension in Proposition 9.4.1 that G_U is the profinite completion of the abstract HNN-extension $\mathrm{HNN}^{abs}(H/U, AU/U, f_U)$. In turn, $\mathrm{HNN}^{abs}(H/U, AU/U, f_U)$ is residually finite (see, e.g., Proposition II.2.12 in Serre [1980]). We deduce that φ_U is a monomorphism. Therefore, $\mathrm{Ker}(\varphi) \leq U$ for every $U \triangleleft_o H$ with $f(A \cap U) = f(A) \cap U$. Hence $\mathrm{Ker}(\varphi) \leq K$.

(2) follows from (1).

(3) Suppose that G is proper. Let $G^{abs} = \mathrm{HNN}^{abs}(H, A, f)$ be the abstract HNN-extension and let X and Y be sets of representatives for H/A and $H/f(A)$, each of them containing 1. Recall that every element g of G^{abs} can be written in a unique way as

$$g = h_1 t^{\epsilon_1} h_2^{\epsilon_2} \cdots h_n^{\epsilon_n} a$$

where $\epsilon_i = \pm 1$, $\epsilon_i = 1$ implies $h_i \in X - \{1\}$, $\epsilon_i = -1$ implies $h_i \in Y - \{1\}$, $h_n \in X - \{1\}$, $a \in A$. From the explicit construction of a profinite HNN-extension (see Proposition 9.4.1) it follows that it suffices to find a normal subgroup N of finite index in G^{abs} such that $N \cap H$ is open in H and $g \notin N$. Since A and $f(A)$ are closed, there is an open normal subgroup U of H such that $a \notin U$, $h_i \notin AU$ and $h_i \notin f(A)U$ for all $i = 1, \dots, n$. Since $\mathrm{HNN}(H, A, f)$ is proper, K is trivial by (2). So we may assume that $f(U \cap A) = f(A) \cap U$. Let ψ be the canonical epimorphism of $G^{abs} = \mathrm{HNN}^{abs}(H, A, t)$ onto $\mathrm{HNN}^{abs}(H/U, AU/U, \bar{f})$, where $\bar{f} : AU/U \longrightarrow f(A)U/U$ is the isomorphism induced by f. Then

$$\psi(g) = \psi(h_1) t^{\epsilon_1} \psi(h_2)^{\epsilon_2} \cdots \psi(h_n)^{\epsilon_n} \psi(a)$$

is written in reduced form (abusing notation, we use t for the image of t). Therefore, $\psi(g)$ is nontrivial. It is known that $\mathrm{HNN}^{abs}(H/U, AU/U, \bar{f})$ is virtually free. Therefore, it contains a normal subgroup of finite index V that intersects H/U trivially and does not contain $\psi(g)$. Then $N = \psi^{-1}(V)$ is the required normal subgroup of G^{abs}.

The converse statement is obvious. □

Next we give a profinite analog of a construction of G. Higman, B. H. Neumann and H. Neumann to show that any countably based profinite group can be embedded into a 2-generated profinite group.

Theorem 9.4.4 *Let L be a countably based profinite group. Then L embeds into some 2-generated profinite group G.*

Proof. Let F be a free profinite group on a basis $\{x_1, x_2\}$ and let σ be the automorphism of F permuting x_1 and x_2. Let N be the closed normal subgroup of F generated by x_1. Then N is free on the topological basis $X = \{x_2^{-\alpha} x_1 x_2^{\alpha} \mid \alpha \in \widehat{\mathbf{Z}}\}$ (see Theorem 8.1.3). Clearly X has countable weight $w(X)$ (see Section 2.6). Choose a clopen neighborhood X_1 of x_1 in X such that $w(X - X_1) = \aleph_0$. Then $\overline{\langle X - X_1 \rangle}$ is a free profinite group of rank $\aleph_0$. Since L is countably based, it can be generated by a countable set converging to 1 (see Propositions 2.4.4 and 2.6.2). Hence, there exists a continuous epimorphism $\varphi : N \longrightarrow L$ such that $\varphi(X_1) = 1$ and $\varphi(\overline{\langle X - X_1 \rangle}) = L$. In particular, $\varphi(x_1) = 1$.

Consider the subgroup $A = N \times \{1\}$ of $F \times L$ and the monomorphism $f : A \longrightarrow F \times L$ defined as follows: $f(a, 1) = (\sigma(a), \varphi(a))$ $(a \in N)$. Then f

is clearly continuous. Consider the profinite HNN-extension $G = \mathrm{HNN}(F \times L, A, f)$. Observe that $f(x_1, 1) = (x_2, 1)$.

We shall first show that $F \times L$ embeds into G, i.e. that $F \times L$ and f satisfy condition (2) in Proposition 9.4.3.

Let U be an open normal subgroup of $F \times L$. Then U contains an open normal subgroup of the form $U_1 \times U_2$ for some $U_1 \triangleleft_o F$, $U_2 \triangleleft_o L$. Since φ is continuous and σ has order 2, one can choose U_1 such that $U_1 \leq \varphi^{-1}(U_2)$ and $\sigma(U_1) = U_1$. Then

$$f(A \cap (U_1 \times U_2)) = \{(\sigma(u), \varphi(u)) \mid u \in N \cap U_1\}$$

and

$$f(A \cap (U_1 \times U_2)) = \{(\sigma(u), \varphi(u)) \mid u \in N \cap \sigma^{-1}(U_1) \cap \varphi^{-1}(U_2)\}.$$

Since $N \cap \sigma^{-1}(U_1) \cap \varphi^{-1}(U_2) = N \cap U_1$, one deduces that $f(A \cap (U_1 \times U_2)) = f(A) \cap (U_1 \times U_2)$, as required.

We now show that G is (topologically) generated by $(x_1, 1)$ and t (see the definition of HNN-extension for the meaning of t). Indeed, conjugating $(x_1, 1)$ by t, we obtain $(x_2, 1)$ and therefore $F \times \{1\} \leq \overline{\langle (x_1, 1), t \rangle}$. This in turn implies that $f(A) \leq \overline{\langle (x_1, 1), t \rangle}$. Since $F \times L = \langle F \times \{1\}, f(A) \rangle$, we have

$$G = \overline{\langle F \times L, t \rangle} = \overline{\langle (x_1, 1), t \rangle},$$

as asserted. □

We finish the section with a modification of Theorem 9.4.4 adapted to the category of abstract groups. This will yield a construction of a residually finite 2-generated torsion-free abstract group whose profinite completion contains every countably based profinite group.

Theorem 9.4.5 *Let $\{g_i \mid i \in \mathbf{N}\}$ be a countable set generators of an abstract group L. Let $\mathcal{N}$ be the family of those normal subgroups of finite index in L which contain all but finitely many of the g_i. Then L embeds into a 2-generated abstract group G, and this embedding induces an embedding of $\mathcal{K}_{\mathcal{N}}(L)$ into $\widehat{G}$. Furthermore, if the natural map $L \longrightarrow \mathcal{K}_{\mathcal{N}}(L)$ is injective, then so is $G \longrightarrow \widehat{G}$.*

Proof. We use the same construction as in Theorem 9.4.4 with small adjustments to our situation. Let F be an abstract free group on a basis $\{x_1, x_2\}$ and let σ be the automorphism of F permuting x_1 and x_2. Let N be the normal subgroup of F generated by x_1. Then N is a free abstract group on the basis $X = \{x_2^{-j} x_1 x_2^j \mid j \in \mathbf{Z}\}$. We can replace X by a new basis Y which converges to 1 with respect to the profinite topology on F, as follows: for any $j > 1$, find the maximal $n \in \mathbf{N}$ with $|j| \geq n!$ and replace $x_1^{x_2^j}$ by $x_1^{x_2^j} x_1^{-x_2^{j_0}}$, where j_0 is the remainder of j modulo $n!$. Then Y converges to 1 (in the profinite topology of F) and $x_1 \in Y$. Choose an epimorphism $\varphi : N \longrightarrow L$ such that $\varphi(Y) = \{g_i \mid i \in \mathbf{N}\}$ and $\varphi(x_1) = 1$. Then φ is continuous if N is regarded as a topological group with the topology induced by the profinite topology of F and L is regarded as a topological group with the topology defined by $\mathcal{N}$. Consider the subgroup $A = N \times \{1\}$ of $F \times L$ and the monomorphism $f : A \longrightarrow F \times L$ defined by $f(a,1) = (\sigma(a), \varphi(a))$, $a \in N$. Then f is clearly continuous with respect to the product topology on $F \times L$. Consider the (abstract) HNN-extension $G = \mathrm{HNN}(F \times L, A, f)$.

Let $\widehat{F}$ be the profinite completion of F. Put $B = f(A)$. Let $\bar{A}$ and $\bar{B}$ be the closures of A and B, respectively, in the profinite group $\widehat{F} \times \mathcal{K}_{\mathcal{N}}(L)$. Let $\bar{f} : \bar{A} \longrightarrow \bar{B}$ be the isomorphism induced by f ($\bar{f}$ can be defined also by the equality $f(a,1) = (\hat{\sigma}(a), \varphi(a))$ ($a \in \bar{N}$), where $\hat{\sigma}$ is the automorphism of $\widehat{F}$ induced by σ and $\bar{\varphi} : \bar{N} \longrightarrow \mathcal{K}_{\mathcal{N}}(L)$ is the epimorphism induced by φ). Consider the profinite HNN-extension $\mathrm{HNN}(\widehat{F} \times \mathcal{K}_{\mathcal{N}}(L), \bar{A}, f)$.

As in the proof of Theorem 9.4.4, one shows that $\widehat{F} \times \mathcal{K}_{\mathcal{N}}(L)$ embeds into $\mathrm{HNN}(\widehat{F} \times \mathcal{K}_{\mathcal{N}}(L), \bar{A}, f)$, i.e., that $\widehat{F} \times \mathcal{K}_{\mathcal{N}}(L)$ and f satisfy condition (2) in Proposition 9.4.3.

To prove the residual finiteness of G, note that the natural embedding $F \times L \longrightarrow \widehat{F} \times \mathcal{K}_{\mathcal{N}}(L)$ induces an embedding of G into $\mathrm{HNN}^{abs}(\widehat{F} \times \mathcal{K}_{\mathcal{N}}(L), \bar{A}, f)$ and the latter group is residually finite by Proposition 9.4.3.

Now we show that the profinite topologies of G and $\mathrm{HNN}(\widehat{F} \times \mathcal{K}_{\mathcal{N}}(L), \bar{A}, \bar{f})$ induce the same topology on $F \times L$. Indeed, let U be a normal subgroup of finite index in G. Then U contains almost all elements of Y. Since $f(U \cap A) = U \cap B$, it follows that U contains almost all g_i. This shows that the topology of G induces a topology on L which is weaker than the one defined by $\mathcal{N}$. It remains to show that for any normal subgroup U_1 of finite index in F and $U_2 \in \mathcal{N}$, there exists a normal subgroup U of finite index in G such that $U \cap (F \times L) \leq U_1 \times U_2$. Choose $U_2 \in \mathcal{N}$. Since φ is continuous and σ has order 2, one can choose U_1 such that $U_1 \leq \varphi^{-1}(U_2)$ and $\sigma(U_1) = U_1$. Then

$$f(A \cap (U_1 \times U_2)) = \{(\sigma(u), \varphi(u)) \mid u \in N \cap U_1\}$$

and

$$B \cap (U_1 \times U_2) = \{(\sigma(u), \varphi(u)) \mid u \in N \cap \sigma^{-1}(U_1) \cap \varphi^{-1}(U_2)\}.$$

Since $N \cap \sigma^{-1}(U_1) \cap \varphi^{-1}(U_2) = N \cap U_1$, one deduces that $f(A \cap (U_1 \times U_2)) = B \cap (U_1 \times U_2)$. Therefore, one has a natural isomorphism

$$\tilde{f} : A(U_1 \times U_2)/(U_1 \times U_2) \longrightarrow B(U_1 \times U_2)/(U_1 \times U_2)$$

and the HNN-extension $\mathrm{HNN}^{abs}(F \times L/(U_1 \times U_2), A(U_1 \times U_2)/(U_1 \times U_2), \tilde{f})$ is an epimorphic image of G. The base subgroup of this extension is finite, and therefore there exists a normal subgroup V of finite index in

$$\mathrm{HNN}(F \times L/(U_1 \times U_2), A(U_1 \times U_2)/(U_1 \times U_2), \tilde{f})$$

that intersects trivially the base subgroup. Let U be the preimage of V in G. Then $U \cap (F \times L) = U_1 \times U_2$, as needed.

Finally, one proves that G is generated by $(x_1, 1)$ and t (see the definition of HNN-extension for the meaning of t) as it was done in the last paragraph of the proof of the preceding theorem. □

Corollary 9.4.6 *There exists a 2-generated residually finite torsion-free abstract group G whose profinite completion $\widehat{G}$ contains an isomorphic copy of every countably based profinite group.*

Proof. It suffices to construct a group G that contains a direct product $K = \prod_n K_n$ of all finite simple groups (one copy for each isomorphism class). Note that by Proposition 4.7.12, for every K_n there exists a finitely generated torsion-free residually finite group Γ_n whose profinite completion contain K_n. Let L be the restricted direct product of the Γ_n (i.e., the subgroup of the direct product consisting of those tuples all whose components are trivial except for a finite number of them). Let X_n be a finite set of generators of Γ_n and $X = \bigcup_{i=1}^{\infty} X_n$. Put $\mathcal{N} = \{N \triangleleft_f L \mid |X - L| < \infty\}$. Then the completion $\mathcal{K}_{\mathcal{N}}(L)$ of L with respect to $\mathcal{N}$ is the direct product $\prod_{i=1}^{\infty} \widehat{\Gamma}_n$. Now Theorem 9.4.5 gives us the required construction for G. Indeed, according to that construction, G is torsion-free since it is an HNN-extension of a torsion free group. □

9.5 Notes, Comments and Further Reading

Throughout this chapter we use freely standard properties of free products, amalgamated products and HNN-extensions of abstract groups. Good sources of information about these properties are Magnus, Karras and Solitar [1966], Lyndon and Schupp [1977] and Serre [1980].

For absolute Galois groups and free pro-$\mathcal{C}$ products, see Pop [1990] (specially Theorem 3.4) and Ershov [1997], where it is proved that the class of absolute Galois groups is closed under free profinite products; see also Koenigsmann [2002] for a simplified proof of this fact and a history of the problem; Mel'nikov [1997]; Efrat and Haran [1994], where an analogous result is proved for absolute Galois groups that are pro-p. In contrast, Koenigsmann [2005] proves that the class of absolute Galois groups is not closed under direct products. See also Efrat [1997].

For a general treatment of cartesian subgroups (Theorem 9.1.6) in a profinite context see Ribes [1990]. Corollary 9.1.7 was proved in a special case in Haran and Lubotzky [1985] and in general in Herfort and Ribes [1989b]. Theorem 9.1.9 was first proved in Binz, Neukirch and Wenzel [1971]; they proved it for a more general type of free product, namely, they allow an infinite set of free factors 'converging' to 1 (see a definition for this type of product in Appendix D, and a simpler proof for the result in Theorem D.3.1).

Proposition 9.1.11 was obtained by Neukirch [1971]; in this paper Neukirch studies applications of free products to Galois theory. Theorem 9.1.12 is proved in Herfort and Ribes [1985]; this paper contains also information about the torsion elements in a free pro-$\mathcal{C}$ product; more precisely, the following result is proved:

Theorem 9.5.1 *Let $G = G_1 \amalg G_2$ be a free pro-$\mathcal{C}$ product and let H be a finite subgroup of G. Then H is conjugate to a subgroup of G_1 or of G_2.*

Proposition 9.1.13 was proved for free profinite groups F of any infinite rank in Herfort and Ribes [1985] and for nonabelian free profinite groups of finite rank in Haran and Lubotzky [1985]. Example 9.1.14 was described by Mel'nikov [1980]. In this paper he also raises the following problem (see Theorem 3.5.15 in this connection).

Open Question 9.5.2 *Is a general inverse limit of a surjective inverse system of free profinite groups of finite rank necessarily a free profinite group?*

Proposition 9.1.15 appears in Lubotzky [1982]. Concerning Remark 9.1.16, the Grushko-Neumann theorem for profinite groups can be reformulated in terms of finite groups (see Ribes and Wong [1991]) as follows: for which extension closed varieties $\mathcal{C}$ of finite groups is it always true that whenever groups G_1, $G_2 \in \mathcal{C}$ are given, then there exists a group $G \in \mathcal{C}$ such that $G_1, G_2 \leq G$, $G = \langle G_1, G_2 \rangle$ and $d(G) = d(G_1) + d(G_2)$? For pro-p groups, the answer is positive (see Proposition 9.1.15); however the result does not hold for general varieties. For the variety of all finite groups Lucchini [2001b] (cf. also Lucchini [1992] and [2001a]) gives bounds for the minimal number of generators of a finite group generated by subgroups of pairwise coprime order. In particular he proves

Theorem 9.5.3 *Let G be a finite group such that $G = \langle G_1, G_2 \rangle$, where G_1 and G_2 are subgroups of G of relatively prime orders. Assume that $d(G_i) \leq r$ $(i = 1, 2)$. Then $d(G) < 2r$, if r is large enough.*

When $\mathcal{C}$ is the class of all finite solvable groups, Kovács and Sim [1991] prove

Theorem 9.5.4 *If a finite solvable group G is generated by s subgroups of pairwise coprime orders, and if each of these subgroups can be generated by r elements, then G can be generated by $r + s - 1$ elements.*

From this one can deduce, for example, that the free prosolvable product $(C_2 \times C_2) \amalg (C_3 \times C_3)$ can be generated by three elements.

Abért and Hedeďűs [2007] contains several results on $d(G)$, where G is the free profinite product of finite groups. In particular they prove that if $G_1, \dots, G_n$ are finite groups and $G = G_1 \amalg \cdots \amalg G_n$ is their free profinite product, then $d(G) \geq n + s' - 1$, where $s' = \max(d(G_i/G_i'))$.

The next question is about the existence of certain Frobenius profinite groups in free profinite products. One can pose the question in terms of normalizers. If A and B are finite groups, then an element in A of order at least 3 cannot normalize an infinite cyclic subgroup of the abstract free product $A * B$. However, it is shown in Herfort and Ribes [1989b] that if the finite groups A and B are solvable, then the free prosolvable product $A \amalg B$ contains Frobenius groups of the form $\widehat{\mathbf{Z}}_\pi \rtimes C$, where C is any finite cyclic subgroup of A, $p \nmid |C|$ for all $p \in \pi$ and C acts fixed-point-free on $\widehat{\mathbf{Z}}_\pi$.

Lemma 9.1.18 and Theorem 9.1.19 were proved by Lubotzky [1982] for free pro-p groups of finite rank, and in general by Ribes [1991]. Theorem 9.1.20 was proved by Lubotzky [1982] for free pro-p groups of finite rank.

In connection with Open Question 9.1.21, we mention the status of the equivalent question for abstract groups. Let F be a free group and let H and K be finitely generated subgroups of F. Put $\mathrm{rk}_{-n}(G) = \max(\mathrm{rank}(G) - n, 0)$. Hanna Neumann conjectured that

$$\mathrm{rk}_{-1}(H \cap K) \leq \mathrm{rk}_{-1}(H)\mathrm{rk}_{-1}(K).$$

The best bound

$$\mathrm{rk}_{-1}(H \cap K) \leq \mathrm{rk}_{-1}(H)\mathrm{rk}_{-1}(K) + \mathrm{rk}_{-3}(H)\mathrm{rk}_{-3}(K),$$

up to now, was obtained recently by Dicks and Formanek [1999].

Exercise 9.1.22 appears in Ribes [1991]. The result in Exercise 9.2.7(1) was obtained by Baumslag [1963]. See Shirvani [1992] for the case when H satisfies a law. Theorem 9.2.4, Exercise 9.2.6 and Examples 9.2.9 and 9.2.10 appear in Ribes [1971], [1973]. Serre (see Ribes [1973]) has also produced examples of nonproper amalgamated free profinite products. A useful necessary and sufficient condition for an amalgamated free pro-p product to be proper is given in Ribes [1971]. The Mayer-Vietoris sequence in Proposition 9.2.13(a) appears in Gildenhuys and Ribes [1974].

Theorem 9.3.1 was proved in Ribes [1974], where it is expressed in terms of cohomology of pairs of groups. Proposition 9.3.8 is proved in Gildenhuys and Ribes [1974]. Theorem 9.3.10 was proved by Neukirch [1971] (in fact he proves this in a more general setting: he allows free products of infinitely many pro-p groups 'converging to 1').

There are two approaches to the task of embedding a countably based profinite (respectively, a residually finite, countably generated) group into a 2-generated profinite (respectively, residually finite) group. The first one, due to J.S. Wilson, is to use the construction of wreath products. This is the method used in Lubotzky and Wilson [1984] (respectively, in Wilson [1980]) to prove Theorem 9.4.4 for extension closed varieties (respectively, a residually finite version of Theorem 9.4.4). The idea of the second approach, due to Z. Chatzidakis, is to use the well-known Higman-Neumann-Neumann construction with certain variations; the approach has been exploited in Chatzidakis [1994], Wilson and Zalesskii [1996] and in Chatzidakis [1999]. This approach allows the control of torsion in the constructed group. Proposition 9.4.3 is due to Chatzidakis [1994], where one can find a proof of Theorem 9.4.4 as well as pro-p versions of Proposition 9.4.3 and Theorem 9.4.4. A pro-p version of Theorem 9.4.5 is proved in Chatzidakis [1999].

There are two examples of 2-generated pro-p groups containing every countably based pro-p group that recently have received attention in the literature. The first one is the Nottingham group, which is a subgroup of finite index of the group $\mathrm{Aut}(\mathbf{F}_p[\![t]\!])$ of ring automorphisms of the power series ring $\mathbf{F}_p[\![t]\!]$ (see Johnson [1988]). The other example is the pro-p completions of 2-generated torsion p-groups constructed by Gupta-Sidki (the construction is similar to Grigorchuk's construction of 3-generated p-groups). Pro-p groups of both types are generated by two elements of order p; these groups are just-infinite (i.e., they do not have infinite proper quotients) and possess many interesting properties (see Camina [1997], Grigorchuk [1980], Gupta and Sidki [1983], Grigorchuk, Herfort and Zalesskii [2000]).

A profinite group G is said to have *bounded generation* if there are elements $x_1, \dots, x_d \in G$, not necessarily different, such that $G = \overline{\langle x_1 \rangle} \cdots \overline{\langle x_d \rangle}$. Let $H = H_1 *_{H_0} H_2$ be a amalgamated free product of abstract groups H_1 and H_2 amalgamating a common subgroup H_0, and let $\widehat{H}$ and $H_{\hat{p}}$ denote the profinite and pro-p completion of H, respectively. The following questions are proposed by A.S. Rapinchuk.

Open Question 9.5.5 *Give (verifiable) sufficient conditions for $\widehat{H}$ to have bounded generation, where $H = H_1 *_{H_0} H_2$.*

An analogous problem (although weaker, due to the fact that pro-p groups with bounded generation are precisely analytic pro-p groups—cf. Lazard [1965]) is

Open Question 9.5.6 *Give (verifiable) sufficient conditions for $H_{\hat{p}}$ to have bounded generation, where $H = H_1 *_{H_0} H_2$.*

For these questions to be meaningful one should of course require in addition that $H = H_1 *_{H_0} H_2$ is residually finite (respectively, residually a finite p-group), or some conditions that insure that $\widehat{H}$ and $H_{\hat{p}}$ do not collapse.

There is a natural analogue of this type of question in an abstract setting; in this case there are known necessary conditions (cf. Fujiwara [2000], Grigorchuk [1996]): if for at least one $i = 1, 2$ the number of double cosets $G_0 \backslash G_i / G_0$ is at least 3, then G does not have bounded generation.

The interest in these questions arises because many S-arithmetic subgroups of algebraic groups associated with quaternion algebras over a number field are amalgamated free products, and progress in these questions would help with the congruence subgroup property for such groups. More information about these questions can be found in Platonov and Rapinchuk [1993], Lubotzky [1995], Rapinchuk [1998].

Finally we indicate two problems suggested by D. Kochloukova involving amalgamated free pro-p products. The problems are suggested by results for abstract free groups that arise in connection with the solution of Tarski's problem on the elementary equivalence of free abstract nonabelian groups (cf. Kharlampovich and Myasnikov [2005] for a source of information on this type of results). Fix a prime p and let G_0 be a free pro-p group of finite rank. Construct pro-p groups G_n recursively as follows. Assume G_n has already been constructed and let R be a procyclic subgroup of G_n with $C_{G_n}(R) = R$; consider a free abelian finitely generated pro-p group $A = R \times B$. Then define the pro-p group G_{n+1} to be the amalgamated free pro-p product

$$G_{n+1} = G_n \amalg_R A.$$

We say that a pro-p group G is a *limit pro-p group* if it is a finitely generated closed subgroup of a group of the form G_n constructed in the above manner.

Open Question 9.5.7 *Let G be a limit pro-p group. Does G satisfy the Howson property? In other words, if H_1 and H_2 are finitely generated closed subgroups of G, is $H_1 \cap H_2$ a finitely generated pro-p group?*

Open Question 9.5.8 *Are limit pro-p groups residually free pro-p?*

Open Question 9.5.9 *Let H be a finitely generated closed subgroup of a limit pro-p group G. Is then H a virtual retract of G, i.e., is there an open subgroup M of G and a normal closed subgroup K of M so that $M = K \rtimes H$?*

Open Questions

We collect here the open questions mentioned in the book. We have maintained the numeration of the original question so that the reader may consult the context in which the question is posed. The wording of the questions are sometimes modified slightly to make them self-contained. We also mention here those open problems that appeared in the first edition of this book which have been solved or advanced in the meantime; in these cases we provide some relevant information.

Open Question 3.5.3 (**Inverse problem of Galois Theory**) *Is every finite group a continuous homomorphic image of the absolute Galois group* $G_{\bar{\mathbf{Q}}/\mathbf{Q}}$ *of the field* $\mathbf{Q}$ *of rational numbers*?

Question in the First Edition of this Book *Let* F *be a free profinite* (*or, more generally, pro*-$\mathcal{C}$) *group on a profinite space* X. *Is there a canonical way of constructing a basis converging to* 1 *for* F? **NOTE:** J-P. Serre has given a negative answer to this question; see Theorem 3.5.13.

Open Question 3.7.2 *What pro*-$\mathcal{C}$ *groups are pro*-$\mathcal{C}$ *completions of finitely generated abstract groups*?

Question in the First Edition of this Book *Let* G *be a finitely generated profinite group. Is every subgroup of finite index in* G *necessarily open*? **NOTE:** This question has been answered positively by N. Nikolov and D. Segal (see Theorem 4.2.2; for a proof see Nikolov and Segal [2007a, 2007b]).

Question in the First Edition of this Book *Let* G *be a finitely generated prosolvable group. Are the terms* (*other than* $[G,G]$) *of the derived series of* G *closed*? **NOTE:** This question has a negative answer; in fact V.A. Roman'kov had already provided a counterexample in 1982 for a more general setting; see Roman'kov [1982].

Open Question 4.8.4 *Let* G *be a finitely generated profinite group and let* n *be a natural number. Let* $\langle G^n\rangle = \langle x^n \mid x \in G\rangle$ *be the abstract subgroup of* G *generated by the* n*-th powers of its elements. Is* $\langle G^n\rangle$ *closed*?

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4,

Open Question 4.8.5b *Is a torsion profinite group necessarily of finite exponent?*

Open Question 6.12.1 *Let G be a solvable pro-p group such that $H^n(G, \mathbf{Z}/p\mathbf{Z})$ is finite for every n. Is G polycyclic?*

Open Question 7.10.1 *For what finite p-groups G does one have $rr(G) = arr(G)$?* [rr = relation rank as a profinite group; arr = relation rank as an abstract group]

Open Question 7.10.4 *Let G be a finitely generated pro-p group such that $cd(G) > 2$ and $\dim H^2(G, \mathbf{Z}/p\mathbf{Z}) = 1$, (i.e., relation rank $rr(G)$ is 1). Does G admit a presentation with a single defining relator of the form u^p?*

Open Question 7.10.5 *Study finitely generated pro-p groups with the following property: every closed subgroup of infinite index is free pro-p.*

Open Question 7.10.6 *Let F be a free pro-p group of finite rank. Is $vcd(\mathrm{Aut}(F))$ finite?*

Question in the First Edition of this Book *Does the Grushko-Neumann theorem hold for free profinite products of profinite groups, that is, if $G = G_1 \amalg G_2$ is the free profinite product of two profinite groups G_1 and G_2, is $d(G) = d(G_1) + d(G_2)$?* **NOTE:** The answer to this is negative. It was answered by A. Lucchini; see Lucchini [2001a, 2001b].

Open Question 9.1.21 *Let F be a free pro-p group and let H and K be closed finitely generated subgroups of F. Is there a bound on the rank of $H \cap K$ in terms of the ranks of H and K?*

Open Question 9.5.2 *Is a general inverse limit of a surjective inverse system of free profinite groups of finite rank necessarily a free profinite group?*

Question in the First Edition of this Book *For which extension closed varieties $\mathcal{C}$ of finite groups is it always true that whenever we are given $G_1, G_2 \in \mathcal{C}$, then there is a group $G \in \mathcal{C}$ such that $G_1, G_2 \leq G$, $G = \langle G_1, G_2 \rangle$ and $d(G) = d(G_1) + d(G_2)$?* **NOTE:** For the class $\mathcal{C}$ of all finite solvable groups the answer is negative, see Kovács and Sim [1991]; for the class $\mathcal{C}$ of all finite groups the answer is negative, see Lucchini [2001a, 2001b].

Question in the First Edition of this Book *Do all profinite Frobenius groups of the form $\widehat{\mathbf{Z}}_\pi \rtimes C$ (C is finite cyclic, $p \nmid |C|$ for all $p \in \pi$ and C acts fixed-point-free on $\widehat{\mathbf{Z}}_\pi$) appear as subgroups of free profinite products $A \amalg B$?* **NOTE:** A positive answer is provided in Guralnick and Haran [2010].

Open Question 9.5.5 *Give (verifiable) sufficient conditions for* $\widehat{H}$ *to have bounded generation, where* $H = H_1 *_{H_0} H_2$.

Open Question 9.5.6 *Give (verifiable) sufficient conditions for* $H_{\hat{p}}$ *to have bounded generation, where* $H = H_1 *_{H_0} H_2$.

Open Question 9.5.7 *Let* G *be a limit pro-*p *group. Does* G *satisfy the Howson property? In other words, if* H_1 *and* H_2 *are finitely generated closed subgroups of* G, *is* $H_1 \cap H_2$ *a finitely generated pro-*p *group?*

Open Question 9.5.8 *Are limit pro-*p *groups residually free pro-*p*?*

Open Question 9.5.9 *Let* H *be a finitely generated subgroup of a limit pro-*p *group* G. *Is then* H *a virtual retract of* G, *i.e., is there an open subgroup* M *of* G *and a normal closed subgroup* K *of* M *so that* $M = K \rtimes H$?

Open Problem C.3.2 *Let* G *be a finitely generated profinite (respectively, pro-*p*) group with finite* $def(G) \geq 2$ *(respectively,* $def_p(G) \geq 2$*). Does* G *contain an open subgroup* U *such that there exists a continuous epimorphism* $U \to F$ *onto a free profinite (respectively, pro-*p*) group* F *of rank at least* 2?

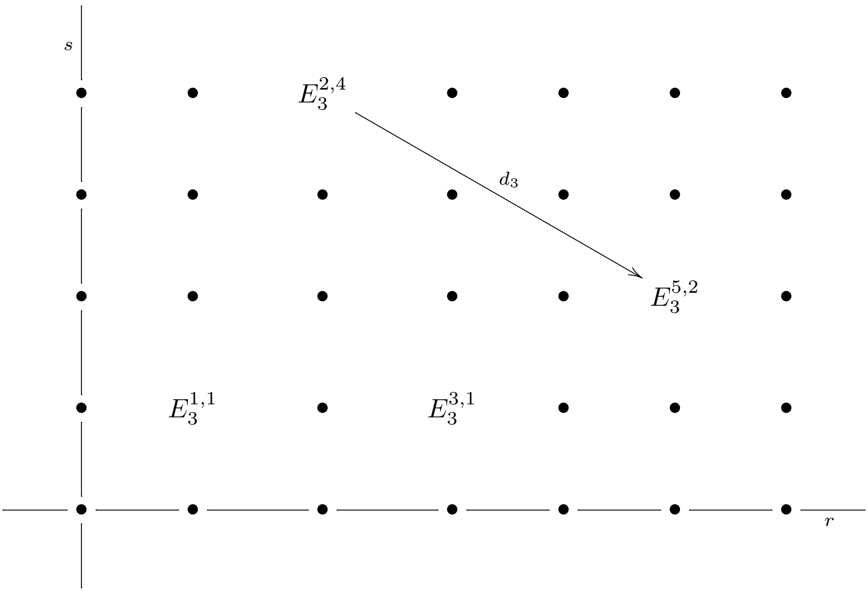
Appendix A: Spectral Sequences

A.1 Spectral Sequences

A *bigraded abelian group* $\mathbf{E}$ is a family $\mathbf{E} = (E^{r,s})_{r,s\in\mathbf{Z}}$ of abelian groups. A *differential* d *of* $\mathbf{E}$ *of bidegree* (p, q) is a family of homomorphisms

$$d : E^{r,s} \to E^{r+p,s+q}$$

such that $dd = 0$.



A *spectral sequence* consists of a sequence $\mathbf{E} = \{\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3, \ldots\}$ of bigraded abelian groups $\mathbf{E}_t = (E_t^{r,s})_{r,s\in\mathbf{Z}}$, with differentials $d_t : \mathbf{E}_t \longrightarrow \mathbf{E}_t$ of bidegree $(t, -t+1)$, such that

$$E_{t+1}^{r,s} \cong \mathrm{Ker}(E_t^{r,s} \xrightarrow{d_t} E_t^{r+t,s-t+1})/\mathrm{Im}(E_t^{r-t,s+t-1} \xrightarrow{d_t} E_t^{r,s}). \qquad (1)$$

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4,

To simplify the notation, from now on we assume that the isomorphism in (1) is in fact an equality. The bigraded abelian group $\mathbf{E}_2$ is called the *initial term* of the spectral sequence.

Lemma A.1.1 *For each $r, s \in \mathbf{Z}$ there exists a series of subgroups of $E_2^{r,s}$*

$$0 = B_2^{r,s} \leq B_3^{r,s} \leq B_4^{r,s} \leq \cdots \leq C_4^{r,s} \leq C_3^{r,s} \leq C_2^{r,s} = E_2^{r,s}$$

such that

$$E_t^{r,s} = C_t^{r,s}/B_t^{r,s} \quad (t \geq 2).$$

Proof. Set $B_2^{r,s} = 0$ and $C_2^{r,s} = E_2^{r,s}$; then $E_2^{r,s} = C_2^{r,s}/B_2^{r,s}$. Define inductively

$$B_{t+1}^{r,s}/B_t^{r,s} = \mathrm{Im}(E_t^{r-t,s+t-1} = C_t^{r-t,s+t-1}/B_t^{r-t,s+t-1} \xrightarrow{d_t} E_t^{r,s} = C_t^{r,s}/B_t^{r,s}),$$

and

$$C_{t+1}^{r,s}/B_t^{r,s} = \mathrm{Ker}(E_t^{r,s} = C_t^{r,s}/B_t^{r,s} \xrightarrow{d_t} E^{r+t,s-t+1} = C_t^{r+t,s-t+1}/B_t^{r+s,s-t+1}).$$

Hence

$$B_2^{r,s} \leq B_t^{r,s} \leq B_{t+1}^{r,s} \leq C_{t+1}^{r,s} \leq C_t^{r,s} \leq C_2^{r,s},$$

and

$$E_{t+1}^{r,s} = (C_{t+1}^{r,s}/B_t^{r,s})/(B_{t+1}^{r,s}/B_t^{r,s}) = C_{t+1}^{r,s}/B_{t+1}^{r,s}.$$ □

Let $C_t^{r,s}$, $B_t^{r,s}$ be as in Lemma A.1.1. Define

$$C_\infty^{r,s} = \bigcap_t C_t^{r,s}, \qquad B_\infty^{r,s} = \bigcup_t B_t^{r,s}$$

and

$$E_\infty^{r,s} = C_\infty^{r,s}/B_\infty^{r,s}.$$

The bigraded abelian group $\mathbf{E}_\infty = (E_\infty^{r,s})_{r,s\in\mathbf{Z}}$, is completely determined by the spectral sequence. We think of the terms $\mathbf{E}_t$ of the spectral sequence as approximating $\mathbf{E}_\infty$.

A *filtered abelian group with filtration F* consists of an abelian group A together with a family of subgroups $F^n(A)$ of A, ($n \in \mathbf{Z}$), such that

$$A \geq \cdots \geq F^n(A) \geq F^{n+1}(A) \geq \cdots.$$

We always assume that a filtration satisfies the additional condition:

$$\bigcup_r F^r(A) = A \quad \text{and} \quad \bigcap_r F^r(A) = 0. \tag{2}$$

To each filtered abelian group A we associate a grading in the following manner

$$G^r(A) = F^r(A)/F^{r+1}(A) \quad (r \in \mathbf{Z}).$$

A *filtered graded abelian group* with filtration F, consists of a family $\mathbf{H} = (H^n)_{n\in\mathbf{Z}}$, of filtered groups H^n.

A spectral sequence $\mathbf{E} = (\mathbf{E}_t)$ is said to *converge* to the filtered graded abelian group $\mathbf{H} = (H^n)$ with filtration F if

$$E_\infty^{r,s} \cong G^r(H^{r+s}) = F^r(H^{r+s})/F^{r+1}(H^{r+s}).$$

We indicate this situation by $E_2^{r,s} \Longrightarrow H^n$ or by $\mathbf{E} \Longrightarrow \mathbf{H}$.

A.2 Positive Spectral Sequences

We say that a spectral sequence $\mathbf{E}$ is *positive* or *first quadrant* if $E_2^{r,s} = 0$, whenever $r < 0$ or $s < 0$. It is clear that if $\mathbf{E}$ is a positive spectral sequence then $E_t^{r,s} = 0$ for $t \geq 2$ and $r < 0$ or $s < 0$. From now on we assume that all spectral sequences are positive.

Proposition A.2.1 *Let* $\mathbf{E}$ *be a positive spectral sequence converging to* $\mathbf{H}$. *Then*

$$\begin{aligned} &\text{(a)} \quad E_t^{r,s} = E_\infty^{r,s} \quad \textit{if } t > \max(r, s+1),\\ &\text{(b)} \quad H^n = 0 \quad \textit{if } n < 0,\\ &\text{(c)} \quad F^r(H^n) = \begin{cases} 0 & \textit{if } r > n,\\ H^n & \textit{if } r \leq 0.\end{cases}\end{aligned}$$

Proof. (a) Note that

$$E_t^{r-t,s+t-1} \xrightarrow{d_t} E_t^{r,s} \xrightarrow{d_t} E_t^{r+t,s-t+1}.$$

If $t > r$, then $E_t^{r-t,s+t-1} = 0$; if $t > s+1$, then $E_t^{r+t,s-t+1} = 0$. So, if $t > \max(r, s+1)$, then $C_t^{r,s} = C_{r+1}^{r,s} = \cdots$, and $B_t^{r,s} = B_{r+1}^{r,s} = \cdots$; hence, by Lemma A.1.1,

$$E_t^{r,s} = E_{t+1}^{r,s} = \cdots = E_\infty^{r,s}.$$

(b) If $r + s = n < 0$, then either $r < 0$ or $s < 0$; so $F^r(H^n)/F^{r+1}(H^n) = E_\infty^{r,s} = 0$; therefore $F^r(H^n) = F^{r+1}H^n$, for all $r \in \mathbf{Z}$; thus $F^r(H^n) = 0$ (since $\bigcap_r F^r H^n = 0$). This implies that $H^n = \bigcup_r F^r(H^n) = 0$.

(c) Let $r + s = n$. Then $E_\infty^{r,s} \cong F^r(H^n)/F^{r+1}(H^n)$. Now, if $r < 0$ or $s < 0$, then $E_\infty^{r,s} = 0$; so $F^r(H^n) = F^{r+1}(H^n)$. Hence,

$$\cdots = F^{-2}(H^n) = F^{-1}(H^n) = F^0(H^n)$$

and

$$F^{n+1}(H^n) = F^{n+2}(H^n) = F^{n+2}(H^n) = \cdots.$$

Thus, it follows from condition (2) that $H^r = F^0(H^n)$ if $r \leq 0$, and $F^r(H^n) = 0$ if $r > n$. □

Proposition A.2.2 *For each n there is a sequence*

$$E_\infty^{n,0} \xrightarrow{\iota} H^n \xrightarrow{\pi} E_\infty^{0,n},$$

where ι is an injection, π a surjection and $\pi\iota = 0$. The sequence is exact if $n = 1$.

Proof. One has the following composition of maps

$$E_\infty^{n,0} \xrightarrow{=} F^n(H^n) \hookrightarrow H^n \longrightarrow H^n/F^1(H^n) \xrightarrow{\cong} E_\infty^{0,n},$$

and so,

$$E_\infty^{n,0} \xrightarrow{\iota} H^n \xrightarrow{\pi} E_\infty^{0,n}.$$

Note that $\operatorname{Im}(\iota) = F^n(H^n) \leq F^1(H^n) = \operatorname{Ker}(\pi)$; hence $\pi\iota = 0$. If $n = 1$, $\operatorname{Im}(\iota) = \operatorname{Ker}(\pi) = F^1(H^n)$, so the sequence is exact. □

The Base Terms

The terms of the form $E_t^{r,0}$ are called the *base terms* of the spectral sequence.

Proposition A.2.3 *For each r there exist epimorphisms*

$$E_2^{r,0} \longrightarrow E_3^{r,0} \longrightarrow \cdots \longrightarrow E_{r+1}^{r,0} \xrightarrow{\cong} E_\infty^{r,0}.$$

Proof. The last arrow is an isomorphism by Proposition A.2.1. Since $E_3^{r,0} \cong \operatorname{Ker}(d_2)/\operatorname{Im}(d_2) = E_2^{r,0}/\operatorname{Im}(d_2)$, we have a surjection $E_2^{r,0} \longrightarrow E_3^{r,0}$. One obtains the other maps in a similar way. □

Each of the maps of Proposition A.2.3 and the map $E_2^{r,0} \longrightarrow E_\infty^{r,0} \xrightarrow{\iota} H^r$ obtained from the maps of Propositions A.2.2 and A.2.3, are called *edge homomorphisms on the base*, and will be denoted by e_B.

The Fiber Terms

The terms of the form $E_t^{0,s}$ are called the *fiber terms* of the spectral sequence.

Proposition A.2.4 *For each s, there exist monomorphisms*

$$E_2^{0,s} \longleftarrow E_3^{0,s} \longleftarrow \cdots \longleftarrow E_{s+2}^{0,s} \xleftarrow{\cong} E_\infty^{0,s}.$$

Proof. The last arrow is an isomorphism by Proposition A.2.1. Since $E_3^{0,s} \cong \operatorname{Ker}(d_2)/\operatorname{Im}(d_2) = \operatorname{Ker}(d_2)$, we have an injection $E_3^{0,s} \longrightarrow E_2^{0,s}$. The other injections are obtained similarly. □

Each of the maps of the Proposition A.2.4, and the map

$$H^s \xrightarrow{\pi} E_\infty^{0,s} \longrightarrow E_2^{0,s}$$

obtained by composing the maps of Propositions A.2.2 and A.2.4, are called *edge homomorphisms on the fiber*, and will be denoted by e_F.

For $n \geq 1$, the homomorphism $d_{n+1} : E_{n+1}^{0,n} \longrightarrow E_{n+1}^{n+1,0}$ is called a *transgression.*

Condition *(*n*).

For a fixed $n \geq 1$, we will say that the spectral sequence $\mathbf{E}$ satisfies condition $^*(n)$ if

$E_2^{r,s} = 0$ whenever $1 \leq s \leq n-1$ and $r+s=n$, and whenever $1 \leq s \leq n-1$ and $r+s=n+1$.

Note that condition $^*(1)$ is vacuous.

Proposition A.2.5 *Assume condition* $^*(n)$ *holds for a positive spectral sequence* $\mathbf{E}$. *Then*

(a) *the monomorphism* $e_F : E_{n+1}^{0,n} \longrightarrow E_2^{0,n}$ *is an isomorphism*;
(b) *the epimorphism* $e_B : E_2^{n+1,0} \longrightarrow E_{n+1}^{n+1,0}$ *is an isomorphism.*

Proof. (a) $E_t^{t,n-t+1} = 0$ if $t \neq n+1$. So $\mathrm{Ker}(d_t : E_t^{0,n} \longrightarrow E_t^{t,n-t+1}) = E_t^{0,n}$ if $t \neq n+1$. Therefore, $E_2^{0,n} \cong E_3^{0,n} \cong \cdots \cong E_{n+1}^{0,n}$.

(b) $E_t^{n-t+1,t-1} = 0$ if $t \neq n+1$. So $\mathrm{Im}(d_t : E_t^{n-t+1,t-1} \longrightarrow E_t^{n+1,0}) = 0$. Therefore, $E_2^{n+1,0} \cong E_3^{n+1,0} \cong \cdots \cong E_{n+1}^{n+1,0}$. □

By the proposition above we can define a map

$$E_2^{0,n} \xrightarrow{e_F^{-1}} E_{n+1}^{0,n} \xrightarrow{d_{n+1}} E_{n+1}^{n+1,0} \xrightarrow{e_B^{-1}} E_2^{n+1,0}$$

if condition $^*(n)$ is satisfied. This homomorphism will also be called a *transgression* and denoted tr.

Theorem A.2.6 *Let* $\mathbf{E} = (E_t^{r,s})$ *be a positive spectral sequence converging to* $\mathbf{H} = (H^n)$. *Assume that* $E_2^{r,s} = 0$ *for* $1 \leq s \leq n-1$ (*for* $n=1$ *this condition is vacuous*). *Then there exists a five term exact sequence*

$$0 \longrightarrow E_2^{n,0} \xrightarrow{e_B} H^n \xrightarrow{e_F} E_2^{0,n} \xrightarrow{tr} E_2^{n+1,0} \xrightarrow{e_B} H^{n+1}.$$

Proof. First notice that

$$\mathrm{Ker}\Big(E_t^{r,0} \xrightarrow{e_B} E_{t+1}^{r,0}\Big) = \mathrm{Im}\Big(E_t^{r-t,t-1} \xrightarrow{d_t} E_t^{r,0}\Big) \quad (3)$$

$$\mathrm{Im}\Big(E_{t+1}^{0,s} \xrightarrow{e_F} E_t^{0,s}\Big) = \mathrm{Ker}\Big(E_t^{0,s} \xrightarrow{d_t} E_t^{t,s-t+1}\Big). \quad (4)$$

We shall prove exactness at each term.

Exactness at $E_2^{n,0}$: It is enough to prove that each $E_t^{n,0} \longrightarrow E_{t+1}^{n,0}$ is an injection ($r = 2, \dots, n$). But this follows from (3) since $E_t^{n-t,t-1} = 0$ ($t = 2, \dots, n$).

Exactness at H^n: Since condition ${}^*(n)$ holds, it follows then from Propositions A.2.2 and A.2.5 that

$$\mathrm{Im}(e_B) = \mathrm{Im}\Big(E_2^{n,0} \longrightarrow H^n\Big) = \mathrm{Im}\Big(E_\infty^{n,0} \xrightarrow{\iota} H^n\Big) = F^n(H^n)$$

and

$$\mathrm{Ker}(e_F) = \mathrm{Ker}\Big(H^n \longrightarrow E_2^{0,n}\Big) = \mathrm{Ker}\Big(H^n \xrightarrow{\pi} E_\infty^{0,n}\Big) = F^1(H^n).$$

Now, by hypothesis, if $n = r + s$ and $1 \le r \le n-1$, then $0 = E_\infty^{r,s} = F^r(H^n)/F^{r+1}(H^n)$; so $F^r(H^n) = F^{r+1}(H^n)$. Hence $F^1(H^n) = F^n(H^n)$. Thus $\mathrm{Im}(e_B) = \mathrm{Ker}(e_F)$.

Exactness at $E_2^{0,n}$: By Proposition A.2.5 and the definition of tr we have

$$\mathrm{Im}(e_F) = \mathrm{Im}\Big(H^n \longrightarrow E_{n+1}^{0,n}\Big) = \mathrm{Im}\Big(E_{n+2}^{0,n} \longrightarrow E_{n+1}^{0,n}\Big),$$

and

$$\mathrm{Ker}(tr) = \mathrm{Ker}\Big(E_{n+1}^{0,n} \longrightarrow E_{n+1}^{n+1,0}\Big).$$

Thus $\mathrm{Im}(e_F) = \mathrm{Ker}(tr)$.

Exactness at $E_2^{n+1,0}$: Analogously,

$$\mathrm{Im}(tr) = \mathrm{Im}\Big(E_{n+1}^{0,n} \longrightarrow E_{n+1}^{n+1,0}\Big),$$

and

$$\mathrm{Ker}(e_B) = \mathrm{Ker}\Big(E_{n+1}^{n+1,0} \longrightarrow H^{n+1}\Big) = \mathrm{Ker}\Big(E_{n+1}^{n+1,0} \longrightarrow E_{n+2}^{n+1,0}\Big).$$

Therefore $\mathrm{Im}(tr) = \mathrm{Ker}(e_B)$. □

Corollary A.2.7 *There exists a five term exact sequence*

$$0 \longrightarrow E_2^{1,0} \xrightarrow{e_B} H^1 \xrightarrow{e_F} B_2^{0,1} \xrightarrow{tr} E_2^{2,0} \xrightarrow{e_B} H^2.$$

Proof. This is a special case of the theorem since for $n = 1$ the hypothesis is vacuous. □

A.3 Spectral Sequence of a Filtered Complex

In this section we study a canonical way of constructing spectral sequences. Given a complex with a suitable filtration, we define a spectral sequence that converges to the filtered graded abelian group consisting of the homology groups of that complex.

Let

$$\mathbf{X} = (\mathbf{X}, \partial) = \cdots \longrightarrow X^{n-1} \xrightarrow{\partial} X^n \longrightarrow X^{n+1} \longrightarrow \cdots$$

be a complex of abelian groups. We say that $\mathbf{X}$ is *filtered* if each X^n has a filtration F compatible with ∂, i.e., for each r and each n, $\partial F^r(X^n) \leq F^r(X^{n+1})$.

Assume that $\mathbf{X}$ is a filtered complex:

$$\begin{array}{ccccc}
\vdots & & \cdots & \vdots & \\
\downarrow & & & \downarrow & \\
X^{n-1} & \geq \cdots \geq & & F^r(X^{n-1}) & \geq \cdots \\
\downarrow & & & \downarrow & \\
X^n & \geq \cdots \geq & & F^r(X^n) & \geq \cdots \\
\downarrow & & & \downarrow & \\
X^{n+1} & \geq \cdots \geq & & F^r(X^{n+1}) & \geq \cdots \\
\downarrow & & & \downarrow & \\
\vdots & & \cdots & \vdots &
\end{array}$$

Then the sequence of homology groups $\mathbf{H} = \{H^n(\mathbf{X})\}$ of this complex can be thought of as a single graded abelian group with a filtration inherited from the filtration of the complex $\mathbf{X}$; namely, $F^r(H^n(\mathbf{X}))$ is the image of $H^n(F^r(\mathbf{X}))$ under the injection $F^r(\mathbf{X}) \hookrightarrow \mathbf{X}$.

Next we begin the construction of a spectral sequence associated to $\mathbf{X}$. Let $r + s = n$ and $r \in \mathbf{Z}$. Set

$$\begin{aligned}
Z_t^{r,s} &= \{a \in F^r(X^n) \mid \partial(a) \in F^{r+t}(X^{n+1})\}, \\
B_t^{r,s} &= \partial Z_{t-1}^{r-t+1,s+t-2} = \partial(F^{r-t+1}(X^{n-1})) \cap F^r(X^n),
\end{aligned}$$

and

$$E_t^{r,s} = Z_t^{r,s}/(B_t^{r,s} + Z_{t-1}^{r+1,s-1}). \tag{5}$$

Since

$$\partial Z_t^{r,s} \leq Z_t^{r+t,s-t+1},$$

and

$$\partial(B_t^{r,s} + Z_{t-1}^{r+1,s-1}) = \partial Z_{t-1}^{r+1,s-1} = B_t^{r+t,s-t+1},$$

we have that the map ∂ induces a homomorphism

$$d_t : E_t^{r,s} \longrightarrow E_t^{r+t,s-t+1}, \tag{6}$$

with $d_t d_t = 0$. Moreover, one checks that

$$\operatorname{Ker}\Big(E_t^{r,s} \xrightarrow{d_t} E_t^{r+t,s-t+1}\Big) = \Big(Z_{t+1}^{r,s} + Z_{t-1}^{r+1,s-1}\Big)\Big/\Big(B_t^{r,s} + Z_{t-1}^{r+1,s-1}\Big),$$

and

$$\operatorname{Im}\left(E_t^{r-t,s+t-1} \xrightarrow{d_t} E_t^{r,s}\right) = \left(B_{t+1}^{r,s} + Z_{t-1}^{r+1,s-1}\right) \Big/ \left(B_t^{r,s} + Z_{t-1}^{r+1,s-1}\right).$$

Hence

$$\begin{aligned} \operatorname{Ker}(d_t)/\operatorname{Im}(d_t) &\cong \left(Z_{t+1}^{r,s} + Z_{t-1}^{r+1,s-1}\right) \Big/ \left(B_{t+1}^{r,s} + Z_{t-1}^{r+1,s-1}\right) \\ &\cong Z_{t+1}^{r,s} \Big/ \left(B_{t+1}^{r,s} + Z_{t-1}^{r+1,s-1}\right) = E_{t+1}^{r,s}. \end{aligned}$$

Observe that this is valid for every $t \in \mathbf{Z}$. Thus we have proved the first part of the following

Theorem A.3.1 *Let $(\mathbf{X}, \partial)$ be a filtered complex. Then*

(a) *There exists a spectral sequence $\mathbf{E}$, where $E_t^{r,s}$ is given by* (5).
(b) *Assume, in addition, that the filtration F of $(\mathbf{X}, \partial)$ is bounded, i.e., for each n there are integers $u = u(n) < v = v(n)$ with $F^u(X^n) = X^n$ and $F^v(X^n) = 0$. Then $\mathbf{E}$ converges to the graded abelian group $\mathbf{H} = H(\mathbf{X})$ (the homology groups of $\mathbf{X}$) with the filtration induced by the filtration of $\mathbf{X}$.*

Proof. (b) To show that $\mathbf{E} \Longrightarrow \mathbf{H}$, we first need to obtain a description of $F^r H^n(\mathbf{X})/F^{r+1}H^n(\mathbf{X})$. Write

$$\begin{aligned} Z_\infty^{r,s} &= \{a \in F^r(X^n) \mid \partial(a) = 0\}, \quad \text{and} \\ B_\infty^{r,s} &= \partial(X^{n-1}) \cap F^r(X^n) \quad (r+s=n). \end{aligned}$$

Then,

$$F^r(H^n(\mathbf{X})) \cong \left(Z_\infty^{r,s} + \partial X^{n-1}\right) \Big/ \partial X^{n-1}.$$

So,

$$\begin{aligned} F^r(H^n(\mathbf{X}))/F^{r+1}(H^n(\mathbf{X})) &\cong \left(Z_\infty^{r,s} + \partial X^{n-1}\right) \Big/ \left(Z_\infty^{r+1,s-1} + \partial X^{n-1}\right) \\ &\cong Z_\infty^{r,s} \Big/ \left[\left(Z_\infty^{r+1,s-1} + \partial X^{n-1}\right) \cap Z_\infty^{r,s}\right] \\ &\cong Z_\infty^{r,s} \Big/ \left(Z_\infty^{r+1,s-1} + B_\infty^{r,s}\right). \end{aligned}$$

Since the filtration of $(\mathbf{X}, \partial)$ is bounded, it is clear that

$$Z_u^{r,s} \cong Z_\infty^{r,s} \quad \text{and} \quad B_u^{r,s} \cong B_\infty^{r,s}$$

for u large enough. Hence

$$F^r(H^n(\mathbf{X}))/F^{r+1}(H^n(\mathbf{X})) \cong E_u^{r,s}$$

for u large enough.

Finally, it is immediate that the boundedness of the filtration of $(\mathbf{X}, \partial)$ implies that $E_u^{r,s} \cong E_\infty^{r,s}$ for u large enough. Thus $\mathbf{E} \Longrightarrow H(\mathbf{X})$. □

A.4 Spectral Sequences of a Double Complex

A *double complex* is a family $\mathbf{K} = (K^{r,s})_{r,s\in\mathbf{Z}}$ of abelian groups together with differentials
$$\partial' : K^{r,s} \to K^{r+1,s}, \qquad \partial'' : K^{r,s} \to K^{r,s+1}$$
such that $\partial'\partial' = 0$, $\partial''\partial'' = 0$ and $\partial'\partial'' + \partial''\partial' = 0$.

Using the double complex $\mathbf{K}$ we define a complex $(\mathbf{X}, \partial) = \mathbf{X} = \mathrm{Tot}(\mathbf{K})$, the *total complex* of $\mathbf{K}$, by

$$X^n = \bigoplus_{r+s=n} K^{r,s},$$

and where $\partial : X^n \longrightarrow X^{n+1}$ is $\partial = \partial' + \partial''$. Note that $(\mathbf{X}, \partial)$ is a complex, for
$$\partial\partial = \partial'\partial' + \partial'\partial'' + \partial''\partial' + \partial''\partial'' = 0.$$

Now we construct in a canonical way two filtrations of its total complex $\mathbf{X}$.

The *first filtration* $'F$ of $\mathbf{X}$ is given by

$$'F^r(X^n) = \bigoplus_{\substack{\alpha+\beta=n \\ \alpha\geq r}} K^{\alpha,\beta}.$$

The *second filtration* $''F$ of $\mathbf{X}$ is defined by

$$''F^s(X^n) = \bigoplus_{\substack{\alpha+\beta=n \\ \beta\geq s}} K^{\alpha,\beta}.$$

For each of these filtrations we can construct corresponding spectral sequences $'\mathbf{E} = ('E_t^{r,s})$ and $''\mathbf{E} = (''E_t^{r,s})$, called the *first* and *second spectral sequence of the double complex* $\mathbf{K}$ (see the construction in Section A.3). Now assume that the double complex $\mathbf{K}$ is positive, i.e., $K^{r,s} = 0$ if $r < 0$ or $s < 0$. Then both the first and second filtrations are bounded. In fact

$$X^n = {'F^0}(X^n) \geq {'F^1}(X^n) \geq \cdots \geq {'F^{n+1}}(X^n) = 0$$

and
$$X^n = {''F^0}(X^n) \geq {''F^1}(X^n) \geq \cdots \geq {''F^{n+1}}(X^n) = 0.$$

So, according to Theorem A.3.1, there exist corresponding spectral sequences $'\mathbf{E} = ('E_t^{r,s})$ and $''\mathbf{E} = (''E_t^{r,s})$ (the first and second spectral sequences of $\mathbf{K}$) converging both of them to $H(\mathbf{X})$ with the induced filtrations.

Next we calculate the initial terms $'\mathbf{E}_2$ and $''\mathbf{E}_2$ of these two spectral sequences. In order to do this we compute first the terms $'\mathbf{E}_1$ and $''\mathbf{E}_1$. We start with the first spectral sequence. We have

$$\begin{aligned} 'Z_1^{r,s} &= \{a \in {'F^r}(X^n) \mid \partial(a) \in {'F^{r+1}}(X^{n+1})\} \\ &\cong \mathrm{Ker}(K^{r,s} \xrightarrow{\partial''} K^{r,s+1}) \oplus {'F^{r+1}}(X^n); \end{aligned}$$

and

$$
\begin{aligned}
{}'B_1^{r,s} + {}'Z_{-1}^{r+1,s-1} &\cong \partial' F^r(X^{n-1}) + {}'F^{r+1}(X^n) \\
&\cong \operatorname{Im}(K^{r,s-1} \xrightarrow{\partial''} K^{r,s}) \oplus {}'F^{r+1}(X^n).
\end{aligned}
$$

Hence

$$
\begin{aligned}
{}'E_1^{r,s} &\cong \operatorname{Ker}\Big(K^{r,s} \xrightarrow{\partial''} K^{r,s+1}\Big)\Big/\operatorname{Im}\Big(K^{r,s-1} \xrightarrow{\partial''} K^{r,s}\Big) \\
&\cong H^s\Big(\cdots \longrightarrow K^{r,s-1} \longrightarrow K^{r,s} \longrightarrow K^{r,s+1} \longrightarrow \cdots\Big) \\
&\cong H^s(K^{r,\bullet}).
\end{aligned}
$$

The mapping $d_1 : {}'E_1^{r,s} \longrightarrow E_1^{r+1,s}$ is induced by ∂', so that

$$
{}'E_2^{r,s} \cong H^r(H^s(K^{i,\bullet}), \partial') = {}'H^r({}''H^s(\mathbf{K})),
$$

where ${}''H$ indicates that we are taking the homology of a vertical complex $K^{i,\bullet}$, and ${}'H$ that we are taking the homology of the horizontal complex of homology groups induced by ∂'.

In a similar manner we obtain for the second spectral sequence

$$
{}''E_1^{r,s} \cong H^s(\cdots \longrightarrow K^{s-1,r} \longrightarrow K^{s,r} \longrightarrow K^{s+1,r} \longrightarrow \cdots) \cong H^s(K^{\bullet,r}),
$$

and

$$
{}''E_2^{r,s} \cong H^r(H^s(K^{\bullet,i}), \partial'') = {}''H^r({}'H^s(\mathbf{K})).
$$

Thus, we have proved the following

Theorem A.4.1 *Let* $\mathbf{K} = (K^{r,s})$ *be a positive double complex.*

(1) *There is a "first spectral sequence"* ${}'\mathbf{E} = ({}'E_t^{r,s})$ *canonically constructed from* $\mathbf{K}$ *such that*

$$
\begin{aligned}
&(\mathrm{a}') \quad {}'E_2^{r,s} \cong {}'H^r({}''H^s(\mathbf{K})), \\
&(\mathrm{b}') \quad {}'E_2^{r,s} \Longrightarrow H^n(\operatorname{Tot}(\mathbf{K})).
\end{aligned}
$$

(2) *There is a "second spectral sequence"* ${}''\mathbf{E} = ({}''E_t^{r,s})$ *canonically constructed from* $\mathbf{K}$ *such that*

$$
\begin{aligned}
&(\mathrm{a}'') \quad {}''E_2^{r,s} \cong {}''H^r({}'H^s(\mathbf{K})), \\
&(\mathrm{b}'') \quad {}''E_2^{r,s} \Longrightarrow H^n(\operatorname{Tot}(\mathbf{K})).
\end{aligned}
$$

A.5 Notes, Comments and Further Reading

This appendix follows the presentation of spectral sequence in Ribes [1970]. For alternative and more detailed presentations see Cartan and Eilenberg [1956], Mac Lane [1963] or McCleary [1985].

Appendix B: A Different Characterization of Free Profinite Groups

B.1 Free vs Projective Profinite Groups

In this appendix we present an additional way of characterizing free pro-$\mathcal{C}$ groups (see Section 3.5). This new characterization emphasizes the difference between free pro-$\mathcal{C}$ groups and projective groups.

A profinite embedding problem for a pro-$\mathcal{C}$ group G

$$\begin{array}{ccc} & & G \\ & & \downarrow{\scriptstyle\varphi} \\ A & \xrightarrow[\alpha]{} & B \end{array} \tag{1}$$

is said to *split* if α splits, i.e., there is a continuous homomorphism $\sigma : B \longrightarrow A$ such that $\alpha\sigma = \mathrm{id}_B$. This means that $A = \mathrm{Ker}(\alpha) \rtimes \sigma(B) \cong \mathrm{Ker}(\alpha) \rtimes B$. If, in addition, α is not an isomorphism, we say that (1) is a *proper split embedding problem* for the pro-$\mathcal{C}$ group G.

Let $\mathfrak{m}$ be an infinite cardinal and let $\mathcal{C}$ be a variety of finite groups. A pro-$\mathcal{C}$ group G is called $\mathfrak{m}$-*quasifree* if for every proper split embedding problem (1) with $A \in \mathcal{C}$, there are exactly $\mathfrak{m}$ distinct epimorphisms

$$\psi : G \longrightarrow A$$

such that $\alpha\psi = \varphi$ (i.e., $\mathfrak{m}$ solutions of the embedding problem).

Proposition B.1.1 *Let G be a pro-$\mathcal{C}$ group and let $d(G) = \mathfrak{m}$ be an infinite cardinal. Then the following conditions are equivalent*

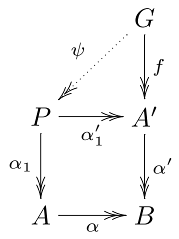
(a) *G is a free pro-$\mathcal{C}$ group of rank $\mathfrak{m}$.*
(b) *G is $\mathcal{C}$-projective and $\mathfrak{m}$-quasifree.*

Proof. Obviously a free pro-$\mathcal{C}$ group is $\mathcal{C}$-projective. By Proposition 3.5.11, it suffices to prove that if (b) holds, every proper embedding problem (1) with $A \in \mathcal{C}$ has precisely $\mathfrak{m}$ different solutions. Assume condition (b), and let (1) be a proper embedding problem for G with $A \in \mathcal{C}$. Since G is $\mathcal{C}$-projective, there exists a continuous homomorphism $f : G \longrightarrow A$ such that $\alpha f = \varphi$. Set $A' = f(G)$, and denote again by f the induced epimorphism $G \longrightarrow A'$. Let $\alpha' : A' \longrightarrow B$ be the restriction of α to A'. Consider the pull-back

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4,

$$P = \{(a, a') \in A \times A' \mid \alpha(a) = \alpha'(a')\}$$

of the maps α and α' (see Section 2.10). Let $\alpha_1 : P \longrightarrow A$ and $\alpha'_1 : P \longrightarrow A'$ be the canonical projections. Observe that α_1 and α'_1 are epimorphisms; furthermore, α'_1 is proper (since $\operatorname{Ker}(\alpha'_1) \cong \operatorname{Ker}(\alpha)$) and splits by means of the section $a' \mapsto (a', a') \quad (a' \in A')$.



By condition (b) there are exactly $\mathfrak{m}$ epimorphisms $\psi : G \longrightarrow P$ such that $\alpha'_1\psi = f$. Each of these ψ determines a solution $\alpha_1\psi$ of the embedding problem (1). We claim that the total number of solutions obtained in this manner of the embedding problem (1) is $\mathfrak{m}$: indeed, suppose that $\psi_i : G \longrightarrow P$ $(i = 1, 2)$ satisfy $\alpha'_1\psi_1 = f = \alpha'_1\psi_2$ and $\alpha_1\psi_1 = \alpha_1\psi_2$; then

$$\alpha\alpha_1\psi_1 = \alpha'\alpha'_1\psi_1 = \alpha'\alpha'_1\psi_2 = \alpha\alpha_1\psi_2,$$

and so $\psi_1 = \psi_2$ by the uniqueness of the universal property of pull-backs. This proves the claim. Finally, since $d(G) = \mathfrak{m}$, the number of continuous homomorphisms from G to A is at most $\mathfrak{m}$, since A is finite. Thus the number of different solutions of the proper embedding problem (1) is exactly $\mathfrak{m}$. □

B.2 Notes, Comments and Further Reading

The concept of $\mathfrak{m}$-quasifree profinite group as well as Proposition B.1.1 appear first in Harbater and Stevenson [2005]. In this paper they give an example of a profinite group that is $\mathfrak{m}$-quasifree but not free profinite. Specifically they prove

Theorem B.2.1 *Let L be any field and let $K = L((x, t))$ be the field of fractions of the ring $L[[x, t]]$ of power series in the indeterminates x and t over the field L. Then the absolute Galois group $G_{\bar{K}/K}$ of K (see Remark 3.5.2) is an $\mathfrak{m}$-quasifree but not free profinite group, where $\mathfrak{m}$ is the cardinal of K.*

For further information about $\mathfrak{m}$-quasifree profinite groups and related concepts, see Appendix D.

Appendix C: Presentations of Profinite Groups

Throughout this appendix $\mathcal{C}$ is an extension closed variety of finite groups.

C.1 Presentations

Let G be a finitely generated pro-$\mathcal{C}$ group with $d(G) = d$. Let $F = F(X)$ be a free pro-$\mathcal{C}$ group on the set X with $|X| = n$ and let

$$1 \longrightarrow K \longrightarrow F \stackrel{\varphi}{\longrightarrow} G \longrightarrow 1 \tag{1}$$

be a short exact sequence of pro-$\mathcal{C}$-groups; we think of K as a subgroup of F. We refer to this sequence as a pro-$\mathcal{C}$ *presentation* of the group G as a pro-$\mathcal{C}$ group. Let R be a set convergent to 1 of topological generators of K as a normal subgroup. Then G is completely determined by X and R, and we write

$$G = \langle X \mid R \rangle. \tag{2}$$

We also refer to $\langle X \mid R \rangle$ as a pro-$\mathcal{C}$ presentation of G. The smallest cardinal $|R|$ among such sets R is denoted $d_F(K)$. If the set R can be chosen to be finite, i.e., $d_F(K) < \infty$, we say that (1) (and (2)) is a finite pro-$\mathcal{C}$ presentation for G, and that G is *finitely presentable* as a pro-$\mathcal{C}$ group. If $\mathrm{rank}(F) = d(G)$, we say that (1) is a *minimal presentation* of G as a pro-$\mathcal{C}$ group. Finally we define the *relation rank* of G as a pro-$\mathcal{C}$ group, written $rr(G)$ or $rr_{\mathcal{C}}(G)$ for emphasis of its dependence on $\mathcal{C}$, to be the smallest $d_F(K)$ for any pro-$\mathcal{C}$ presentation of G.

The following proposition shows that in some strong sense pro-$\mathcal{C}$ presentations of a pro-$\mathcal{C}$ group are essentially unique.

Proposition C.1.1 *Let G be a finitely generated pro-$\mathcal{C}$ group with $d(G) = d \leq m \leq n < \infty$ and let $F = F_{\mathcal{C}}(n)$ be the free pro-$\mathcal{C}$ group of rank n.*

(a) *Let*

$$\varphi : F \longrightarrow G$$

be a continuous epimorphism. Then there exists a basis

$$\{x_1, \dots, x_m, x_{m+1}, \dots, x_n\}$$

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4,

of F such that $\varphi(x_{m+1}) = \cdots = \varphi(x_n) = 1$. Consequently, if we put $F_1 = \overline{\langle x_1, \ldots, x_m \rangle}$, the restriction $\varphi_{|F_1} : F_1 \longrightarrow G$ is an epimorphism from the free pro-$\mathcal{C}$ group F_1 onto G; and if $m = d$, this defines a minimal pro-$\mathcal{C}$ presentation for G.

(b) *Let*

$$1 \longrightarrow K_i \longrightarrow F \xrightarrow{\varphi_i} G \longrightarrow 1 \quad (i = 1, 2)$$

be two pro-$\mathcal{C}$ presentations of the group G. Then there exists an automorphism $\tau : F \longrightarrow F$ of F such that $\varphi_1 = \varphi_2 \tau$; consequently, $\tau(K_1) = K_2$. In particular $d_F(K_1) = d_F(K_2)$.

Proof. (a) Say $G = \overline{\langle z_1, \ldots, z_m \rangle}$. According to Proposition 2.5.4, there exist $x_1, \ldots, x_n$ such that $F = \overline{\langle x_1, \ldots, x_n \rangle}$ and $\varphi(x_i) = z_i$, if $i = 1, \ldots, m$, while $\varphi(x_i) = 1$, if $i = m+1, \ldots, n$. Observe that $\{x_1, \ldots, x_n\}$ is a basis for F by Lemma 3.3.5(b).

(b) Choose a basis $x_1, \ldots, x_n$ of F. By Proposition 2.5.4 and Lemma 3.3.5(b), there exists a basis $y_1, \ldots, y_n$ of F such that $\varphi_2(y_i) = \varphi_1(x_i)$ for all $i = 1, \ldots, n$. Define τ to be the unique automorphism of F such that $\tau(x_i) = y_i$ for all $i = 1, \ldots, n$. □

Corollary C.1.2 *Let G be a finitely generated pro-$\mathcal{C}$ group.*

(a) *Let*

$$1 \longrightarrow K_1 \longrightarrow F_1 \xrightarrow{\varphi_1} G \longrightarrow 1, \qquad 1 \longrightarrow K_2 \longrightarrow F_2 \xrightarrow{\varphi_2} G \longrightarrow 1$$

be pro-$\mathcal{C}$ presentations of G such that $\mathrm{rank}(F_1) \leq \mathrm{rank}(F_2) < \infty$; *then $d_{F_1}(K_1) \leq d_{F_2}(K_2)$.*

(b) *If $1 \longrightarrow K \longrightarrow F \longrightarrow G \longrightarrow 1$ is a minimal presentation as a pro-$\mathcal{C}$ group. Then*

$$rr(G) = d_F(K).$$

Proof. Part (b) follows immediately from (a). To prove part (a), let $\mathrm{rank}(F_1) = n_1$ and $\mathrm{rank}(F_2) = n_2$. By Proposition C.1.1(a), there exists a basis

$$\{x_1, \ldots, x_{n_1}, x_{n_1+1}, \ldots, x_{n_2}\}$$

such that $\varphi_2(x_{n_1+1}) = \cdots = \varphi_2(x_{n_2}) = 1$. Consider the closed normal subgroup N of F_2 generated by $x_{n_1+1}, \ldots, x_{n_2}$. Since $\varphi_2(N) = 1$, the corresponding sequence

$$1 \longrightarrow K_2/N \longrightarrow F_2/N \longrightarrow G \longrightarrow 1$$

is exact. Obviously $d_{F_2/N}(K_2/N) \leq d_{F_2}(K_2)$. Since $F_2/N \cong F_1$, the result follows from Proposition C.1.1(b). □

The dependency of the relation rank on the class $\mathcal{C}$ is expressed by

Proposition C.1.3 *Let $\mathcal{C}' \subseteq \mathcal{C}$ be extension closed varieties of finite groups and let G be a finitely generated pro-$\mathcal{C}'$ group. Then $rr_{\mathcal{C}'}(G) \leq rr_{\mathcal{C}}(G)$.*

Proof. Let

$$1 \longrightarrow K \longrightarrow F \xrightarrow{\varphi} G \longrightarrow 1$$

be a minimal pro-$\mathcal{C}$ presentation of G. Then (see Proposition 3.4.2)

$$1 \longrightarrow K/R_{\mathcal{C}'}(F) \longrightarrow F/R_{\mathcal{C}'}(F) \xrightarrow{\varphi} G \longrightarrow 1$$

is a minimal pro-$\mathcal{C}'$ presentation of G. Since $d_{F/R_{\mathcal{C}'}(F)}(K/R_{\mathcal{C}'}(F)) \leq d_F(K)$, the result follows from Corollary C.1.2(b). □

Exercise C.1.4 Let

$$0 \longrightarrow K \longrightarrow F_{\mathcal{C}}(n) \longrightarrow F_{\mathcal{C}}(m) \longrightarrow 0$$

be an exact sequence. Prove that $d_{F_{\mathcal{C}}(n)}(K) = n - m$.

Lemma C.1.5 *Let $L = K \rtimes H$ be a semidirect product of profinite groups. Assume that $\{x_1, \ldots, x_n\}$ is a set of topological generators of L. Let $x_i = k_i h_i$ $(k_i \in K, h_i \in H, i = 1, \ldots, n)$. Then $\{k_i \mid i = 1, \ldots, n\}$ is a set of topological generators of K as a normal subgroup.*

Proof. Let N be generated by $\{k_1, \ldots, k_n\}$ as a closed normal subgroup of L. Then $L = NH = KH$, $N \leq K$ and $N \cap H = L \cap H = 1$. So, $N = K$. □

Example C.1.6 Finitely presented groups

(a) Let $G \in \mathcal{C}$. Then obviously $d_F(G) < \infty$ for every presentation (1). In particular G is finitely presentable as a pro-$\mathcal{C}$ group.
(b) Let G be a finitely generated projective profinite group with $d(G) = d$. Then G is finitely presentable as a profinite group and $rr(G) \leq d$. Indeed, if $F(d)$ denotes the free profinite group of rank d, then $F(d) = K \rtimes G$, where K is some closed normal subgroup of $F(d)$. So the statement follows from Lemma C.1.5.
(c) Let $F_{\mathcal{C}}(n)$ be the free pro-$\mathcal{C}$ group of finite rank n. Then $F_{\mathcal{C}}(n)$ is finitely presentable as a profinite group and $rr(F_{\mathcal{C}}(n)) \leq n$. Indeed, since $\mathcal{C}$ is extension closed, $F_{\mathcal{C}}(n)$ is a projective profinite group (see Proposition 7.6.7); so this is a special case of (a).

Proposition C.1.7 *Let $1 \longrightarrow K \longrightarrow F \longrightarrow G \longrightarrow 1$ be a pro-$\mathcal{C}$ presentation of a finitely generated pro-$\mathcal{C}$ group G. Assume that $K \neq 1$ and $K = \overline{[K, K]}$. [This is the case, for example, if G is a free prosolvable group of finite rank and the presentation above is a minimal profinite presentation: see Exercise 8.2.8(3)]. Then $d_F(K) = 1$. Consequently G admits a pro-$\mathcal{C}$ presentation with a single defining relator.*

Proof. Let $M(K)$ be the intersection of all maximal closed normal subgroups R of K. Since K does not have nontrivial finite abelian quotients, $K/M(K) = \prod_{R \in \mathcal{M}} K/R$, where each K/R is a finite nonabelian simple group (see Lemma 8.2.3). Choose an element $k \in K$ such that its natural projection in K/R is nontrivial, for all $R \in \mathcal{M}$. Let N denote the normal subgroup of F generated by k. Then $NM(K)/M(K) = K/M(K)$ (see Lemma 8.2.4(b)); so $NM(K) = K$. Therefore, by Proposition 8.3.6, $N = K$; i.e., K is generated by k as a normal subgroup; thus, since K is nontrivial, $d_F(K) = 1$. □

Exercise C.1.8 Let G be a finitely generated pro-$\mathcal{C}$ group. Then G is finitely presentable as a profinite group if an only if it is finitely presentable as a pro-$\mathcal{C}$ group.

C.2 Relation Modules

Given a pro-$\mathcal{C}$ presentation (1) of a finitely generated pro-$\mathcal{C}$ group G, put $K' = \overline{[K,K]}$, the commutator subgroup of K; and let

$$\tilde{K} = K/K'$$

denote its corresponding abelian pro-$\mathcal{C}$ quotient. Then

$$1 \longrightarrow \tilde{K} = K/K' \longrightarrow F/K' \longrightarrow G \longrightarrow 1$$

is an exact sequence of pro-$\mathcal{C}$ groups. Let $\sigma : G \longrightarrow F$ be a continuous section of φ as topological spaces (see Proposition 2.2.2). Define a right action of G on $\tilde{K}$ by

$$(kK', g) \mapsto (kK')^{\sigma(g)K'} = \sigma(g)^{-1}k\sigma(g)K'.$$

One checks easily that this action is well-defined (independent of the choice of the continuous section σ) and it is continuous. Hence $\tilde{K} = K/K'$ becomes a profinite $[\![\mathbf{Z}_{\hat{\mathcal{C}}}G]\!]$-module, which is called the *relation module* corresponding to the presentation (1). The smallest cardinality of a set of generators of the module $\tilde{K}$ is denoted by $d_G(\tilde{K})$. Clearly

$$d_G(\tilde{K}) \leq d_F(K).$$

Proposition C.2.1 *Let G be a finitely generated pro-$\mathcal{C}$ group and let*

$$1 \longrightarrow K \longrightarrow F \xrightarrow{\varphi} G \longrightarrow 1$$

be a pro-$\mathcal{C}$ presentation of G. Then

$$d_F(K) = \begin{cases} 1 & \text{if } K \neq 1 \text{ and } \tilde{K} = 0; \\ d_G(\tilde{K}) & \text{otherwise.} \end{cases}$$

Furthermore, if $K = 1$, $d_F(K) = 0 = d_G(\tilde{K})$.

Proof. The last statement is obvious. If $K \neq 1$ and $\tilde{K} = 0$, the result is just Proposition C.1.7. So, we may assume then that $K \neq 1$ and $\tilde{K} \neq 0$. If $d_G(\tilde{K}) = \infty$, then obviously $d_F(K) = \infty$. Therefore, we may assume in addition that $d_G(\tilde{K}) = r < \infty$.

Since $d_G(\tilde{K}) \leq d_F(K)$, it suffices to show that $d_F(K) \leq r$. Let $\mathcal{M}$ be the collection of all maximal closed normal subgroups R of K, and let $M(K) = \bigcap_{R \in \mathcal{M}} R$. By Lemma 8.2.2, there exist subsets $\mathcal{N}_s$ and $\mathcal{N}_a$ of $\mathcal{M}$ such that

$$K/M(K) = K_s \times K_a,$$

where $K_s = \prod_{R \in \mathcal{N}_s} K/R$ and for each $R \in \mathcal{N}_s$, K/R is a nonabelian finite simple group, and $K_a = \prod_{R \in \mathcal{N}_a} K/R$ and for each $R \in \mathcal{N}_a$, K/R is an abelian simple group. Hence K_a is a nontrivial $[\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]$-module which in fact is a quotient of the $[\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]$-module $\tilde{K}$; so K_a can be generated by at most r elements as a $[\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]$-module.

Let $y_1, \ldots, y_r \in K$ be such that their images in K_a generate K_a as a $[\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]$-module. And let $y \in K$ be such that its image in each K/R is nontrivial, for all $R \in \mathcal{N}_s$. Let T be the smallest closed normal subgroup of F containing the r elements $yy_1, y_2, \ldots, y_r$. Then, $TM(K)/M(K)$ contains K_s by Lemma 8.2.4(a), and hence it contains K_a. Therefore, $TM(K)/M(K) = K/M(K)$; so $TM(K) = K$. Hence $T = K$, according to Proposition 8.3.6, and thus $d_F(K) \leq r$, as needed. □

Proposition C.2.2 *Let*

$$1 \longrightarrow N \longrightarrow F(n) \xrightarrow{\varphi} G \longrightarrow 1 \tag{3}$$

and

$$1 \longrightarrow M \longrightarrow F(m) \xrightarrow{\psi} G \longrightarrow 1$$

be pro-$\mathcal{C}$ presentations of a finitely generated pro-$\mathcal{C}$ group G, and let $n > m$. Put $\tilde{M} = M/M'$ and $\tilde{N} = N/N'$. Then

$$\tilde{N} = [\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]^{n-m} \oplus \tilde{M},$$

as $[\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]$-modules.

Proof. We may assume that there exists a basis $\{x_1, \ldots, x_m, x_{m+1}, \ldots, x_n\}$ of $F(n)$ such that $\varphi(x_{m+1}) = \cdots = \varphi(x_n) = 1$, $F(m) = \overline{\langle x_1, \ldots, x_m \rangle}$ and $\psi = \varphi_{|F(m)}$ (see Proposition C.1.1). Hence the presentation (3) can be rewritten in the form

$$1 \longrightarrow N \longrightarrow F(n) = F(m) \amalg F(n-m) \xrightarrow{\varphi} G \longrightarrow 1,$$

where $\amalg$ indicates free pro-$\mathcal{C}$ product, and with certain abuse of notation, $F(m) = \overline{\langle x_1, \ldots, x_n \rangle}$ and $F(n-m) = \overline{\langle x_{m+1}, \ldots, x_n \rangle}$; moreover $\varphi_{|F(m)} = \psi$. Denote by T the smallest closed normal subgroup of $F(n)$

containing $F(n-m)$. Then $N = TM = T \rtimes M$, so that $\tilde{N} = T/T' \oplus \tilde{M}$. It remains to prove that $T/T' \cong [\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]^{n-m}$. To see this recall that T is the free pro-$\mathcal{C}$ group on the basis

$$B = \{fx_if^{-1} \mid i = m+1, \dots, n \text{ and } f \in F(n-m)\}$$

(see Proposition 9.1.23). Therefore, T/T' is a free $\mathbf{Z}_{\hat{\mathcal{C}}}$-module on the same basis B. Now that action of G on $\tilde{N}$ described above induces an action on B which can be described as follows: $(fx_if^{-1}, g) \mapsto \tilde{g}(fx_if^{-1})\tilde{g}^{-1}$, where $\tilde{g} \in F(n-m)$ and $\varphi(\tilde{g}) = g$. Clearly this action of G on B is a free action and the quotient of B under this action is $\{x_{m+1}, \dots, x_n\}$. Thus, according to Proposition 5.7.1(a), T/T' is a free profinite $[\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]$-module on $B/G = \{x_{m+1}, \dots, x_n\}$; i.e., $T/T' \cong [\![\mathbf{Z}_{\hat{\mathcal{C}}} G]\!]^{n-m}$, as needed. □

Next we study the *deficiency*

$$d - d_{F(n)}(K)$$

of the pro-$\mathcal{C}$ presentation (1). As we shall see in the next theorem, the deficiency is independent of the presentation for most groups G, but not for all of them. The case of a minimal presentation plays a crucial role in this study. For a finitely generated pro-$\mathcal{C}$ group G with $d = d(G)$ and a minimal pro-$\mathcal{C}$ presentation

$$1 \longrightarrow D \longrightarrow F(d) \xrightarrow{\varphi} G \longrightarrow 1,$$

denote the corresponding relation module by

$$A_{\mathcal{C}}(G) = \tilde{D} = D/D'.$$

We use $A(G)$ for the relation module of a minimal profinite presentation of G, and if G is a pro-p group, we write $A_p(G)$ instead of $A_{\mathcal{C}}(G)$, where $\mathcal{C}$ is the variety of all finite p-groups. Observe that if G is a pro-p group and (1) is a pro-p presentation of G, then $\tilde{K} = 0$ if and only if $K = 0$, since K is a free pro-p group. Hence if $\mathcal{C}$ consists only of finite p-groups, only parts (a) and (b) of the following theorem are relevant (see Proposition 7.8.4).

Theorem C.2.3 *Let G be a finitely generated pro-$\mathcal{C}$ group and put $d = d(G)$. We continue with the above notation. Consider a pro-$\mathcal{C}$ presentation*

$$1 \longrightarrow N \longrightarrow F(n) \xrightarrow{\varphi} G \longrightarrow 1$$

of G.

(a) *If $A_{\mathcal{C}}(G) \neq 0$, then*

$$n - d_{F(n)}(N) = d - d_{F(d)}(D), \quad \textit{for all } n \geq d;$$

(*note that $d_{F(d)}(D)$ might not be finite*).

(b) *If* $A_{\mathcal{C}}(G)=0$ *and* $G=F(d)$*, then*

$$n-d_{F(n)}(N)=d, \quad \textit{for all } n\geq d.$$

(c) *If* $A_{\mathcal{C}}(G)=0$ *and* $G\neq F(d)$*, then*

$$n-d_{F(n)}(N)=d, \quad \textit{for all } n>d \quad \textit{and} \quad d-d_{F(d)}(D)=d-1.$$

Proof. By Proposition C.2.2,

$$d_G(\tilde{N})=n-d+d_G(\tilde{D}). \tag{4}$$

So, $\tilde{N}\neq 0$ if either $A_{\mathcal{C}}(G)=\tilde{D}\neq 0$ or $n>d$.

(a) In this case $\tilde{N}\neq 0$ for all $n\geq d$. Hence $d_{F(n)}(N)=d_G(\tilde{N})$ for all $n\geq d$, according to Proposition C.2.1. Thus

$$d_{F(n)}(N)=n-d+d_{F(d)}(D)$$

as desired.

(b) In this case we also have $d_{F(n)}(N)=d_G(\tilde{N})$ for all $n\geq d$, but in addition $d_{F(d)}(D)=0$. Thus $n-d_{F(n)}(N)=d$.

(c) In this case $\tilde{N}\neq 0$, and so $d_{F(n)}(N)=d_G(\tilde{N})$, if $n>d$. Hence from (4) and the assumption $d_G(\tilde{D})=0$, we deduce that $n-d_{F(n)}(N)=d$, if $n>d$. Finally, according to Proposition C.2.1, $d_{F(d)}(D)=1$; hence $d-d_{F(d)}(D)=d-1$. □

We define the *deficiency* $def_{\mathcal{C}}(G)$ of a finitely generated pro-$\mathcal{C}$ group G, in the category of pro-$\mathcal{C}$ groups, to be the maximum of $n-r$, where $n=|X|<\infty$, $r=|R|$ and $\langle X \mid R\rangle$ ranges over all pro-$\mathcal{C}$ presentations of G. If $\mathcal{C}$ is the class of all finite groups, we simply write $def(G)$; and write $def_p(G)$ if $\mathcal{C}$ is the variety of all finite p-groups. In view of Theorem C.2.3,

$$def_{\mathcal{C}}(G)=n-d_{F(n)}(N)$$

where $1\longrightarrow N\longrightarrow F(n)\longrightarrow G\longrightarrow 1$ is any pro-$\mathcal{C}$ presentation of G, unless $A_{\mathcal{C}}(G)=0$, in which case, $def_{\mathcal{C}}(G)=d(G)$.

Observe that $def_{\mathcal{C}}(G)$ is finite if and only if G is finitely presentable. One deduces from Theorem 7.8.5 that if G is a finite p-group, $def_p(G)\leq 0$.

We end this section with an alternative internal characterization of those pro-$\mathcal{C}$ groups G satisfying the condition $A_{\mathcal{C}}(G)=0$.

Lemma C.2.4 *Let*

$$1\longrightarrow D\longrightarrow F(d)\xrightarrow{\varphi} G\longrightarrow 1$$

be a minimal pro-$\mathcal{C}$ *presentation of a finitely generated pro-*$\mathcal{C}$ *group* G *with* $d(G)=d$*. Then*

$$A_{\mathcal{C}}(G)=D/D'=0$$

if and only if whenever $H \leq_o G$, *then*

$$H/H' \cong \mathbf{Z}^r_{\hat{\mathcal{C}}},$$

the free abelian pro-$\mathcal{C}$ *group of rank* r, *where* $r = 1 + (d-1)[G : H]$.

Proof. To simplify the notation, put $F = F(d)$. Assume $A_{\mathcal{C}}(G) = D/D' = 0$. Let $H \leq_o G$ and define $r = 1 + (d-1)[G : H]$. We need to show that $H/H' \cong \mathbf{Z}^r_{\hat{\mathcal{C}}}$. To see this, identify G with F/D and H with $\ddot{H}/D$, where $D \leq \ddot{H} \leq_o F$. Then $[F : \ddot{H}] = [G : H]$, and so $\ddot{H}$ is a free pro-$\mathcal{C}$ group of rank $r = 1 + (d-1)[G : H]$ (see Theorem 3.6.2). Since $D = D'$, $\ddot{H}' \geq D$; hence

$$H/H' = (\ddot{H}/D)/(\ddot{H}'/D) = \ddot{H}/\ddot{H}' \cong \mathbf{Z}^r_{\hat{\mathcal{C}}},$$

as desired.

Conversely, assume that whenever $H \leq_o G$, then $H/H' \cong \mathbf{Z}^r_{\hat{\mathcal{C}}}$, where $r = 1 + (d-1)[G : H]$. We need to show that $D = D'$. Suppose on the contrary that $D \neq D'$. Again identify G with F/D. Since $D' \triangleleft_c F$ and $D \neq D'$, there exists some $L \triangleleft_o F$ such that $D' \leq L \cap D < D$. Put $T = LD$. Then $H = T/D$ is open in $G = F/D$; moreover, $[G : H] = [F : T]$. By assumption $\mathbf{Z}^r_{\hat{\mathcal{C}}} \cong H/H' \cong T/T'D$. Since T is a free pro-$\mathcal{C}$ group of rank $r = 1 + (d-1)[G : H]$ (see Theorem 3.6.2), we deduce that $T/T' \cong \mathbf{Z}^r_{\hat{\mathcal{C}}}$. So (see Proposition 2.5.2), the natural epimorphism $T/T' \longrightarrow T/T'D$ is an isomorphism, a thus $D \leq T'$. However, since $T/L \cong D/(L \cap D)$ is abelian and nontrivial, we have that $T' \leq L$; hence $T' \cap D \leq L \cap D < D$, a contradiction. Thus $D = D'$, as desired. □

Exercise C.2.5 With the notation of Lemma C.2.4, prove that $A_{\mathcal{C}}(G) = 0$ if and only if $D = \mathcal{R}_{\mathcal{S}_{\mathcal{C}}}(D)$ (see Section 3.4 for this notation), where $\mathcal{S}_{\mathcal{C}}$ is the variety of solvable groups that are in $\mathcal{C}$.

C.3 Notes, Comments and Further Reading

The material in this appendix follows Lubotzky [2001]. This paper contains also a description of $rr(G)$ in cohomological terms. A finite group G is called *quasisimple* if it is perfect and simple modulo its center; in Guralnick, Kantor, Kassabov and Lubotzky [2007] it is proved that such a group has a profinite presentation with two generators and at most 18 relators. Furthermore, they prove that, as profinite groups, $rr(A_n)$, $rr(S_n) \leq 4$, for every n.

Hillman and Schmidt [2008] prove that if G is a finitely presentable pro-p group which contains a finite nontrivial normal subgroup, then $def_p(G) \leq 0$; while if G contains a nontrivial finitely generated closed normal subgroup N, then $def_p(G) \leq 1$. In this last case, when $def_p(G) = 1$, they show that $cd(G) = 2$, N is a free pro-p group, and either $N \cong \mathbf{Z}_p$ or G/N is virtually $\mathbf{Z}_p$.

In Grunewald, Jaikin-Zapirain, Pinto and Zalesskii [2008] a profinite version of this last result is given:

Theorem C.3.1 *Let G be a finitely presentable profinite group of positive deficiency and N a finitely generated normal subgroup such that the p-Sylow subgroup $(G/N)_p$ is infinite and p divides the order of N. Then either the p-Sylow subgroup of G/N is virtually cyclic or the p-Sylow subgroup of N is cyclic. Moreover, $cd_p(G) = 2$, $cd_p(N) = 1$ and $vcd_p(G/N) = 1$.*

The following problem is suggested by A. Lubotzky as an analogue of result for abstract groups in Baumslag and Pride [1978].

Open Problem C.3.2 *Let G be a finitely generated profinite (respectively, pro-p) group with finite $def(G) \geq 2$ (respectively, $def_p(G) \geq 2$). Does G contain an open subgroup U such that there exists a continuous epimorphism* $U \to F$ onto a free profinite (respectively, pro-p) group F of rank at least 2?

Appendix D: Wreath Products and Some Subgroup Theorems

Throughout this appendix $\mathcal{C}$ is an extension closed variety of finite groups.

In this appendix we present alternative proofs of the structure of subgroups of certain type of profinite groups. The common thread is that these proofs are based on wreath products; they are simpler than the original proofs, some of them presented previously in this book and, more importantly, these are direct proofs which do not rely on corresponding results for abstract groups. In fact, in some cases, the same method of proof presented here can be used for the corresponding result for abstract groups with the advantage that this proof is conceptually simpler (for example, the Kurosh subgroup theorem for free products of groups).

We use the following notation and conventions. Composition of maps in this appendix is always assumed to be right-to-left, except when dealing with permutations in a symmetric group S_Σ, which we multiply left-to-right. Let $K \leq L$ be pro-C group groups. If $x, y \in L$, we define $x^y = y^{-1}xy$, ${}^yx = yxy^{-1}$ and $K^y = y^{-1}Ky$. The inner automorphism inn_y of L determined by y is the automorphism $x \mapsto yxy^{-1}$ $(x \in L)$.

D.1 Permutational Wreath Products

Fix a finite set Σ. Given a group pro-$\mathcal{C}$ group A, define A^Σ to be the (pro-$\mathcal{C}$) group of all functions $f\colon \Sigma \longrightarrow A$. We write the argument of such a function f on its right; thus the operation on A^Σ is given by

$$(fg)(s) = f(s)g(s) \quad (f, g \in A^\Sigma, s \in \Sigma).$$

We denote by $\delta\colon A \to A^\Sigma$ the *diagonal homomorphism*: it assigns to $a \in A$, the constant function $\delta_a \in A^\Sigma$ defined by $\delta_a(s) = a$, for all $s \in \Sigma$. Note that δ is continuous. The image of δ is denoted δ_A.

Assume that a pro-$\mathcal{C}$ group G acts continuously on Σ on the right. Define the *permutational wreath product* $A \wr G$ (with respect to the G-set Σ) to be the semidirect product

$$A \wr G = A^\Sigma \rtimes G,$$

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4,

where the action of G on A^Σ is on the left and it is defined by $(g, f) \mapsto {}^g f$, and

$${}^g f(s) = f(sg) \quad (g \in G, f \in A^\Sigma, s \in \Sigma).$$

Since this action is continuous and both A and G are pro-$\mathcal{C}$ groups, so is $A \wr G$. We sometimes denote the elements of $A \wr G = A^\Sigma \rtimes G$ by (f, g) or $f \cdot g$ or fg, with $f \in A^\Sigma, g \in G$, depending on convenience. Observe that G centralizes δ_A in $A \wr G$, so that $\delta_A G = \delta_A \times G$.

Several fundamental properties of the wreath product are recorded in the following proposition.

Proposition D.1.1

(a) *If $B \leq A$ and $H \leq G$ are pro-$\mathcal{C}$ groups, then*

$$B \wr H = B^\Sigma \rtimes H \leq_c A \wr G = A^\Sigma \rtimes G.$$

(b) *Functoriality on A: $(-) \wr G$ is a functor, i.e., for each continuous homomorphism $\alpha: A \longrightarrow B$, there is a continuous homomorphism*

$$\alpha \wr G: A \wr G = A^\Sigma \rtimes G \longrightarrow B \wr G = B^\Sigma \rtimes G$$

given by $(f, g) \mapsto (\alpha f, g)$ $(f \in A^\Sigma, g \in G)$ so that

(b1) $\mathrm{id}_A \wr G = \mathrm{id}_{A \wr G}$, *and*

(b2) *if $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ are continuous homomorphisms of pro-$\mathcal{C}$ groups, then*

$$\beta\alpha \wr G = (\beta \wr G)(\alpha \wr G).$$

(c) *Furthermore, $\alpha \wr G$ is an epimorphism (respectively, monomorphism) if and only if α is an epimorphism (respectively, monomorphism).*

Let H be an open subgroup of a pro-$\mathcal{C}$ group G. Let $\Sigma = H \backslash G$ be the set of all right cosets of H in G. Denote by

$$\rho: G \longrightarrow S_\Sigma$$

the regular representation of G in S_Σ, i.e., ρ is the homomorphism defined by $\rho(g) = \bar{g}$ $(g \in G)$, where $\bar{g}: \Sigma \to \Sigma$ is the permutation $Hx \mapsto Hxg$ $(x \in G)$. Note that

$$\mathrm{Ker}(\rho) = \bigcap_{x \in G} xHx^{-1} = H_G,$$

the core of H in G. So $H_G \triangleleft_o G$. Therefore ρ is continuous.

Fix a right transversal T of H in G, i.e., a complete set of representatives of the right cosets Hx $(x \in G)$. We denote the representative of Hx in T by either t_{Hx} or $\bar{x}$, as convenient. Define $s_T \in G^\Sigma$ to be the map that assigns to each right coset of H in G its representative in T:

$$s_T(Hx) = t_{Hx} = \bar{x} \in T \quad (x \in G).$$

Consider the monomorphism of groups $\widetilde{\varphi}: G \to G \wr \rho(G)$ given by the composition of homomorphisms

$$G \xrightarrow{\delta\times\rho} \delta_G \times \rho(G) \hookrightarrow G \wr \rho(G) \xrightarrow{\mathrm{inn}_{s_T}} G \wr \rho(G)\ .$$

Explicitly, if $g \in G$, then

$$\widetilde{\varphi}(g) = s_T(\delta_g \cdot \rho(g))s_T^{-1} = f_g \cdot \rho(g),$$

where $f_g \in G^{\Sigma}$ is defined by $f_g = s_T {\delta_g}^{\rho(g)}(s_T^{-1})$, i.e.,

$$f_g(Hx) = t_{Hx} g t_{Hxg}^{-1} \quad (x \in G).$$

We remark that $\widetilde{\varphi}(G) \le H \wr \rho(G)$, because $f_g(Hx) = t_{Hx} g t_{Hxg}^{-1} \in H$ $(x \in G)$. Furthermore, $\tilde{\varphi}$ is continuous. Therefore, we have proved

Theorem D.1.2 (Embedding Theorem) *Let G be a pro-$\mathcal{C}$ group and let H be an open subgroup of G.*

(a) *There is a continuous injective homomorphism $\varphi: G \longrightarrow H \wr \rho(G)$ defined by*

$$\varphi(g) = f_g \cdot \rho(g)$$

where $f_g: \Sigma = H\backslash G \longrightarrow H$ is given by $f_g(Hx) = t_{Hx} g t_{Hxg}^{-1}$ $(g, x \in G)$.

(b) *$\varphi(H) \le H^{\Sigma} \rtimes \rho(H) = H \wr \rho(H)$.*

We record the following facts for future use; they follow by routine computation in the wreath product.

Lemma D.1.3 *Let G and A be pro-$\mathcal{C}$ groups. Consider an open subgroup H of G and set $\Sigma = H\backslash G$. Let $\psi: G \longrightarrow A \wr \rho(G) = A^{\Sigma} \rtimes \rho(G)$ be a continuous homomorphism such that*

$$\begin{array}{ccc} G & \xrightarrow{\ \psi\ } & A \wr \rho(G) \\ & {\scriptstyle\rho}\searrow & \downarrow{\scriptstyle\theta} \\ & & \rho(G) \end{array}$$

commutes, where θ is the projection. Put $\psi(g) = (\tilde{f}_g, \rho(g))$ $(g \in G)$. Then the following hold:

(a) $\tilde{f}_{g_1 g_2 \cdots g_n} = \tilde{f}_{g_1} {}^{\rho(g_1)}\tilde{f}_{g_2} \cdots {}^{\rho(g_1 \cdots g_{n-1})}\tilde{f}_{g_n}$, *for $g_1, \dots, g_n \in G$;*

(b) $\tilde{f}_{g^{-1}} = ({}^{\rho(g^{-1})}\tilde{f}_g)^{-1} = {}^{\rho(g^{-1})}(\tilde{f}_g^{-1})$, *for $g \in G$.*

Remark If $H \triangleleft_o G$, then Σ has the structure of a pro-$\mathcal{C}$ group that we denote K. Identifying K with its canonical image in $S_{\Sigma} = S_K$, we have $K = \rho(G)$, so that $\varphi: G \hookrightarrow H \wr K$. This is the so called Kaluznin-Krasner

Theorem in the context of profinite groups: every finite extension of a pro-$\mathcal{C}$ group H by a pro-$\mathcal{C}$ group K can be embedded in $H \wr K$.

From now on we shall use the notation $T = \{t_1, \dots, t_k\}$, and we shall assume that $t_1 = 1$ is the representative of the coset H, i.e., $t_H = t_1 = 1$. Then the action of $H^{t_i} = t_i^{-1} H t_i$ on $\Sigma = H \backslash G$ fixes the element $Ht_i \in \Sigma$. Hence if A is a group and $f \in A^\Sigma$, one has ${}^{\rho(x)}f(Ht_i) = f(Ht_i)$, for all $x \in H^{t_i}$. Therefore, the copy

$$\{f(Ht_i) \mid f \in A^\Sigma\} \cong A$$

of the group A corresponding to the $Ht_i \in \Sigma$ component of the direct product A^Σ centralizes $\rho(H^{t_i})$ in $A \wr \rho(H^{t_i})$. Thus

$$A \wr \rho(H^{t_i}) = A^\Sigma \rtimes \rho(H^{t_i}) = A \times (A^{\Sigma - \{Ht_i\}} \rtimes \rho(H^{t_i})).$$

We denote by $\pi_{A,i}\colon A \wr \rho(H^{t_i}) \to A$ the corresponding projection:

$$\pi_{A,i}(f \cdot \rho(x)) = f(Ht_i) \quad (x \in H^{t_i}, f \in A^\Sigma).$$

The case $i = 1$ will be used so often, that it is convenient to set $\pi_A = \pi_{A,1}$. Part (b) of the following lemma expresses the naturality of $\pi_{A,i}$.

Lemma D.1.4 *We continue with the above setting. Let $i \in \{1, \dots, k\}$.*

(a) *There is a commutative diagram*

$$\begin{array}{ccc} H^{t_i} & \xrightarrow{\varphi_{|H^{t_i}}} & H \wr \rho(H^{t_i}) \\ & {\scriptstyle \mathrm{inn}_{t_i |H^{t_i}}} \searrow & \downarrow {\scriptstyle \pi_{H,i}} \\ & & H. \end{array}$$

In particular, for $i = 1$, $\pi_H \varphi_{|H} = \pi_{H,1} \varphi_{|H} = \mathrm{id}_H$.

(b) *If $\alpha\colon A \longrightarrow B$ is a homomorphism of groups, then the diagram*

$$\begin{array}{ccc} A \wr \rho(H^{t_i}) & \xrightarrow{\alpha \wr \rho(H^{t_i})} & B \wr \rho(H^{t_i}) \\ {\scriptstyle \pi_{A,i}} \downarrow & & \downarrow {\scriptstyle \pi_{B,i}} \\ A & \xrightarrow[\alpha]{} & B \end{array}$$

commutes.

(c) *One has $\bigcap_{i=1}^k (A \wr \rho(H^{t_i})) = A \wr \rho(H_G) = A^\Sigma$, where H_G is the core of H in G. The restriction $(\pi_{A,i})_{|A^\Sigma}\colon A^\Sigma \to A$ is the usual direct product projection.*

Proof. To prove (a) observe that, for $r \in H^{t_i}$, one has

$$\pi_{H,i}\varphi(r) = f_r(Ht_i) = t_{Ht_i} r t_{Ht_i r}^{-1} = t_i r t_i^{-1}$$

since H^{t_i} stabilizes Ht_i. The proof of (b) follows directly from the definitions of $\pi_{A,i}$, $\pi_{B,i}$, and $\alpha \wr \rho(H^{t_i})$. Part (c) is clear, as $\bigcap_{i=1}^k H^{t_i} = H_G = \mathrm{Ker}\rho$. $\square$

D.2 The Nielsen-Schreier Theorem for Free Pro-$\mathcal{C}$ Groups

We present an elementary proof of part of Theorem 3.6.2 using wreath products; namely we prove that open subgroups of free pro-$\mathcal{C}$ groups are free pro-$\mathcal{C}$. Our proof is algebraic in nature and proceeds by direct verification of the universal property without appeal to the corresponding result for abstract free groups. Let $F = F(X, *)$ be a free pro-$\mathcal{C}$ group on a pointed profinite space $(X, *)$ and let H be an open subgroup of F. Then (see Proposition 3.3.13), F contains a copy of the abstract free group $\Phi = \Phi(Y)$ on the set $Y = X - \{*\}$, as a dense subgroup.

Elements of Φ can be viewed as reduced words over $Y \cup Y^{-1}$. Recall that a *Schreier transversal* for $\Delta \leq \Phi$ is a right transversal T of Δ in Φ which is closed under taking prefixes (and in particular contains the empty word): if $y_1, \ldots, y_n \in Y \cup Y^{-1}$ and $y_1 \cdots y_i \cdots y_n \in T$ is a word in reduced form, then $y_1 \cdots y_i \in T$, for all $i = 0, \ldots, n-1$. The existence of Schreier transversals is a standard exercise in Zorn's Lemma. We include a proof here for completeness.

Lemma D.2.1 *There exists a Schreier transversal T of Δ in Φ.*

Proof. Consider the collection $\mathcal{P}$ of all prefix-closed sets of reduced words in $Y \cup Y^{-1}$ that intersect each right coset of Δ in at most one element; order $\mathcal{P}$ by inclusion. Then $\{1\} \in \mathcal{P}$, so $\mathcal{P} \neq \emptyset$. It is also clear that the union of a chain of elements from $\mathcal{P}$ is again in $\mathcal{P}$, hence $\mathcal{P}$ has a maximal element T by Zorn's Lemma. We need to show that each right coset of H has a representative in T. Suppose this is not the case and choose a word w of minimum length so that $Hw \cap T = \emptyset$. Since $1 \in T$, it follows $w \neq 1$ and hence $w = uy$ is in reduced form where $y \in Y \cup Y^{-1}$. By assumption on w, we have $Hu = Ht$ some $t \in T$. If ty is reduced as written, then $T \uplus \{ty\} \in \mathcal{P}$, contradicting the maximality of T. If ty is not reduced as written, then $ty \in T$ by closure of T under prefixes, and $Hw = Hty$, contradicting the choice of w. This completes the proof that T is a transversal. □

We now proceed with our proof of Theorem 3.6.2 via wreath products.

Theorem D.2.2 *Open subgroups of free pro-$\mathcal{C}$ groups are free pro-$\mathcal{C}$. More precisely, let F be a free pro-$\mathcal{C}$ group on a profinite pointed space $(X, *)$ and let H be an open subgroup of F. Let Φ be the free abstract group on $Y = X - \{*\}$ and let T be a Schreier transversal for $H \cap \Phi$ in Φ. Define*

$$B = \{tx(\overline{tx})^{-1} \mid (t, x) \in T \times X\}. \tag{1}$$

Then $1 \in B$, B is a profinite space and H is a free pro-$\mathcal{C}$ on the pointed space $(B, 1)$.

Proof. Observe that the natural map

$$(H \cap \Phi)\backslash\Phi \longrightarrow H\backslash F = \Sigma$$

is a bijection, and T is a right transversal for H in F. Clearly $1 \in B$. The map

$$T \times X \longrightarrow B = \{tx(\overline{tx})^{-1} \mid t \in T, x \in X\} \subseteq H \leq F$$

given by

$$(t, x) \mapsto tx(\overline{tx})^{-1} = tx(t_{\pi(tx)})^{-1}$$

(where $\pi: F \to \Sigma = H\backslash F$ is the projection) is continuous, since π and the section $Hf \mapsto t_{Hf}$ from $H\backslash F$ to F are obviously continuous. Therefore B is closed by the compactness of $T \times X$, i.e., B is profinite.

Our goal is to show that any continuous map $\alpha: B \longrightarrow G$ of pointed spaces, with G a pro-$\mathcal{C}$ group, extends uniquely to a continuous homomorphism $\gamma: H \longrightarrow G$. Denote by Σ the set $H\backslash F$ of right cosets of H in F and let $\rho: F \to S_\Sigma$ be the associated permutation representation of F.

To motivate our construction of the extension, we start with a proof of uniqueness. Let $\gamma: H \longrightarrow G$ be any continuous homomorphism extending α. Consider the standard wreath product embedding $\varphi: F \longrightarrow H \wr \rho(F)$ of Theorem D.1.2. The functoriality of the wreath product and Lemma D.1.4 yield the commutative diagram

$$\begin{array}{ccccc}
F & \xrightarrow{\ \varphi\ } & H \wr \rho(F) & \xrightarrow{\ \gamma\wr\rho(F)\ } & G \wr \rho(F) \\
\uparrow & & \uparrow & & \uparrow \\
H & \xrightarrow{\ \varphi_{|H}\ } & H \wr \rho(H) & \xrightarrow{\ \gamma\wr\rho(H)\ } & G \wr \rho(H) \\
& \searrow^{\mathrm{id}_H} & \downarrow{\scriptstyle \pi_H} & & \downarrow{\scriptstyle \pi_G} \\
& & H & \xrightarrow[\ \gamma\ ]{} & G
\end{array}$$

Hence γ is uniquely determined by $(\gamma\wr\rho(F))\varphi$, which is in turn determined by its values on X. But if $x \in X$, then $(\gamma \wr \rho(F))\varphi(x) = (\gamma f_x, \rho(x))$. Now recall that

$$f_x(Hw) = t_{Hw}xt_{Hwx}^{-1} \in B$$

and hence $\gamma f_x = \alpha f_x$. Thus the unique possible extension of α to a homomorphism is given by $\pi_G(\tau_{|H})$ where $\tau: F \longrightarrow G \wr \rho(F)$ is the homomorphism defined on X by $\tau(x) = (\alpha f_x, \rho(x))$. Let us show $\pi_G(\tau_{|H})$ extends α.

Let $b \in B$. Then $b = tx(\overline{tx})^{-1}$, for some $t \in T$, $x \in X$. Let us suppose that

$$t = x_1 \cdots x_{k-1} \quad \text{and} \quad (\overline{tx})^{-1} = x_{k+1} \cdots x_n$$

in reduced form. We put $x_k = x$ so that $b = x_1 \cdots x_n$, although this product may not be reduced as written. Set $t_i = \overline{x_1 \cdots x_i}$, for $i = 0, \ldots, n$. Using that Schreier transversals are prefix-closed, one easily deduces the formulas:

$$t_i = \begin{cases} x_1 \cdots x_i, & \text{if } i < k, \\ x_n^{-1} \cdots x_{i+1}^{-1}, & \text{if } i > k. \end{cases} \tag{2}$$

Indeed, the first formula is clear. The second follows because, for $i \geq k+1$, $Ht_i = Htxx_{k+1} \cdots x_i = Hx_n^{-1} \cdots x_{k+1}^{-1} x_{k+1} \cdots x_i = Hx_n^{-1} \cdots x_{i+1}^{-1}$.

Our aim now is to verify $\pi_G \tau(b) = \alpha(b)$. Put $\tau(r) = (f'_r, \rho(r))$, for $r \in F$. We claim that if $t_{Hw} x t_{Hwx}^{-1} = 1$ ($x \in X \cup X^{-1}, w \in F$), then $f'_x(Hw) = 1$. This is immediate if $x \in X$, since $f'_x = \alpha f_x$ and $f_x(Hw) = t_{Hw} x t_{Hwx}^{-1}$. Next assume $x \in X^{-1}$. Hence, taking into account that $x^{-1} \in X$,

$$f'_x(Hw) = (\alpha f_{x^{-1}}(Hwx))^{-1} = (\alpha(t_{Hwx} x^{-1} t_{Hw}^{-1}))^{-1} = 1,$$

since $t_{Hwx} x^{-1} t_{Hw}^{-1} = (t_{Hw} x t_{Hwx}^{-1})^{-1} = 1$.

In light of (2) it follows that $t_{i-1} x_i t_i^{-1} = 1$ for all $i \neq k$. Thus by the claim and Lemma D.1.3,

$$\begin{aligned} \pi_G \tau(b) &= f'_b(H) = f'_{x_1 \cdots x_n}(H) \\ &= f'_{x_1}(H) f'_{x_2}(Hx_1) \cdots f'_{x_n}(Hx_1 \cdots x_{n-1}) \\ &= f'_{x_1}(Ht_0) f'_{x_2}(Ht_1) \cdots f'_{x_n}(Ht_{n-1}) \\ &= f'_{x_k}(Ht_{k-1}) = \alpha(t_{k-1} x_k t_k^{-1}) = \alpha(b), \end{aligned}$$

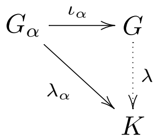
as needed. □

Remark that the above proof only shows that B is a basis for H. It does not follow from the proof that $B - \{1\}$ is in bijection with the set of pairs $(t, x) \in T \times (X - \{*\})$ satisfying $tx(\overline{tx})^{-1} \neq 1$ (and hence the formula in Theorem 3.6.2(b)). However this can be deduced by a straightforward independent combinatorial reasoning.

D.3 The Kurosh Subgroup Theorem for Profinite Groups

In this section we prove an enhanced version of Theorem 9.1.9. Again the point here is that this new proof is based on wreath products and it is not dependent on the corresponding theorem for abstract groups. Indeed this new proof is elementary and, as one easily sees, it provides a proof for the abstract case with essentially the same procedure.

First we define a more general concept of 'free pro-$\mathcal{C}$ product' than the one used in Section 9.1. Let G be a pro-$\mathcal{C}$ group and let $\{G_\alpha \mid \alpha \in A\}$ be a collection of pro-$\mathcal{C}$ groups indexed by a set A. For each $\alpha \in A$, let $\iota_\alpha : G_\alpha \longrightarrow G$ be a continuous homomorphism. One says that the family $\{\iota_\alpha \mid \alpha \in A\}$ is *convergent* if whenever U is an open neighborhood of 1 in G, then U contains all but a finite number of the images $\iota_\alpha(G_\alpha)$. We say that G together with the ι_α is the *free pro-$\mathcal{C}$ product* of the groups G_α if the following universal property is satisfied: whenever $\{\lambda_\alpha : G_\alpha \longrightarrow K \mid \alpha \in A\}$ is a convergent family of continuous homomorphisms into a pro-$\mathcal{C}$ group K, then there exists a unique continuous homomorphism $\lambda: G \longrightarrow K$ such that



commutes, for all $\alpha \in A$. One easily sees that if such a free product exists, then the maps ι_α are injections. We denote such a free pro-$\mathcal{C}$ product again by

$$G = \coprod_{\alpha \in A}{}^{r} G_\alpha.$$

Free pro-$\mathcal{C}$ products exist and are unique. To construct the free pro-$\mathcal{C}$ product G one proceeds as follows: let

$$G^{abs} = *_{\alpha \in A} G_\alpha$$

be the free product of the G_α as abstract groups. Consider the pro-$\mathcal{C}$ topology on G^{abs} determined by the collection of normal subgroups N of finite index in G^{abs} such that $G^{abs}/N \in \mathcal{C}$, $N \cap G_\alpha$ is open in G_α, for each $\alpha \in A$, and $N \geq G_\alpha$, for all but finitely many α. Put

$$G = \varprojlim_N G/N.$$

Then G together with the maps $\iota_\alpha : G_\alpha \longrightarrow G$ is the free pro-$\mathcal{C}$ product $\coprod^r_{\alpha \in A} G_\alpha$.

If the set A is finite, the 'convergence' property of the homomorphisms ι_α is automatic; in that case, instead of $\coprod^r$, we use the symbol $\coprod$ as in Section 9.1.

For such free products, one has the following analogue of the Kurosh Subgroup Theorem

Theorem D.3.1 *Let H be an open subgroup of the free pro-$\mathcal{C}$ product*

$$G = \coprod_{\alpha \in A}{}^{r} G_\alpha.$$

Then, for each $\alpha \in A$, there exists a set D_α of representatives of the double cosets $H \backslash G / G_\alpha$ such that the family of inclusions

$$\{uG_\alpha u^{-1} \cap H \hookrightarrow H \mid u \in D_\alpha, \alpha \in A\}$$

converges, and H is the free pro-$\mathcal{C}$ product

$$H = \left[\coprod_{\alpha \in A, u \in D_\alpha}^{r} uG_\alpha u^{-1} \cap H \right] \amalg F,$$

where F is a free pro-$\mathcal{C}$ group of finite rank.

Before dealing with the actual proof of the theorem we make a reduction to the case when A is finite. Consider the core $H_G = \bigcap_{g \in G} gHg^{-1}$ of H in G. Since H is open, so is H_G. Hence, by definition, there exists a finite subset B of A such that $G_\alpha \le H_G$ for all $\alpha \in A - B$. Let G' be the closed subgroup of G generated by the groups $\{G_\alpha \mid \alpha \in A - B\}$; then one sees that $G' = \coprod_{\alpha \in A-B}^{r} G_\alpha$; consequently

$$G = \left[\coprod_{\alpha \in B} G_\alpha \right] \amalg G'$$

is a free pro-$\mathcal{C}$ product of finitely many factors, and one easily sees that it suffices to prove the theorem for this product: indeed, observe first that for all $\alpha \in A - B$, $H_G \ge G_\alpha$ and since $H_G \triangleleft G$, one has $HuG_\alpha = Hu = HuG'$ ($u \in G$), i.e., $H \backslash G / G' = H \backslash G = H \backslash G / G_\alpha$; on the other hand,

$$uG'u^{-1} \cap H = uG'u^{-1} = \coprod_{\alpha \in A-B} uG_\alpha u^{-1} = \coprod_{\alpha \in A-B} (uG_\alpha u^{-1} \cap H).$$

Hence from now on we shall assume that A is a finite indexing set, and we write it as $A = \{1, \dots, n\}$.

As pointed out in Proposition 9.1.8, the natural homomorphism

$$G^{abs} = G_1 * \cdots * G_n \longrightarrow G = G_1 \amalg \cdots \amalg G_n$$

is a continuous injection; in fact we may think of G^{abs} as a dense subgroup of G. Let $H \le_o G$ and define $H^{abs} = G^{abs} \cap H$. We have $[G : H] = [G^{abs} : H^{abs}]$ (this is a variation of Proposition 3.2.2); one easily deduces that a right transversal of H^{abs} in G^{abs} is also a right transversal of H in G. Similarly, a set of representatives of the double cosets $H^{abs} \backslash G^{abs} / G_\alpha$ is also a set of representatives of the double cosets $H \backslash G / G_\alpha$. We use these facts to define certain special sets of representatives of the double cosets $H \backslash G / G_\alpha$ and of the right cosets $H \backslash G$ so that those representatives are in fact in G^{abs}. To do this we take advantage of the well-known fact that the elements g of G^{abs} can be written uniquely as products $g = g_1 g_2 \cdots g_m$ where each g_i belongs to some G_α ($\alpha \in A$) and $g_i \in G_\alpha$ implies $g_{i+1} \notin G_\alpha$, for $i = 1, \dots, m-1$ (cf. Lyndon and Schupp [1977], Ch. IV). The number m will be called the *syllable length* of g and we write $\ell(g) = m$. If $S \subseteq G$, denote by $\ell(S)$ the smallest syllable length of an element of S. By convention, the syllable length of the identity is 0. If $g_m \in G_\alpha$, then we shall say that g ends in the syllable α or that α is the last syllable of g.

Kurosh Systems

Let us begin by setting up additional notation. Let $\{H_i \mid i \in I\}$, be the right cosets of H and assume there is a symbol $1 \in I$ such that $H_1 = H$. Assume that we have a transversal (with elements in G^{abs}) T_α of the right cosets of H in G for each $\alpha \in A$. Denote by $\alpha(H_i)$ the representative of H_i in T_α. We require $\alpha(H) = 1$, all $\alpha \in A$.

A collection $D = \{D_\alpha \mid \alpha \in A\}$ of systems D_α of representatives $\alpha(HgG_\alpha) \in G^{abs}$ of the double cosets $H\backslash G/G_\alpha$, $(\alpha \in A)$, together with a system $\{T_\alpha \mid \alpha \in A\}$ of transversals (with elements in G^{abs}) for $H\backslash G$ is called a *Kurosh system* if the following holds:

(i) If $g = \alpha(HgG_\alpha)$, then $g = \alpha(Hg)$;
(ii) $\alpha(HgG_\alpha)$ is either 1 or ends in a syllable $\beta \neq \alpha$;
(iii) $H_i \subseteq HgG_\alpha$ and $\alpha(HgG_\alpha) = g$ implies $\alpha(H_i) \in gG_\alpha$;
(iv) If $1 \neq g = \alpha(HgG_\alpha)$ has last syllable in G_β, then $\beta(Hg) = g$;
(v) $\ell(\alpha(HgG_\alpha)) = \ell(HgG_\alpha)$.

Proposition D.3.2 *Kurosh systems exist.*

Proof. We proceed by induction on the length of the double cosets HgG_α. If $\ell(HgG_\alpha) = 0$, i.e., $HgG_\alpha = HG_\alpha$ choose $\alpha(HgG_\alpha) = 1$ and $\alpha(H) = 1$; if $H \neq H_i \subseteq HG_\alpha$, choose $a_\alpha \in G_\alpha$ so that $H_i = Ha_\alpha$, and put $\alpha(H_i) = a_\alpha$. Then conditions (i)–(v) hold. Let $n > 1$, and assume representatives $\beta(HrG_\beta)$ and $\beta(H_i)$ have been chosen whenever $H_i \subseteq HrG_\beta$ and $\ell(HrG_\beta) \leq n-1$ $(\beta \in A, r \in G)$, satisfying conditions (i)–(v). Let $\ell(HgG_\alpha) = n$ with $\ell(g) = n$. Then $g = \tilde{g}a_\beta$, where $\ell(\tilde{g}) = n-1$, $1 \neq a_\beta \in G_\beta$ and $\beta \neq \alpha$. Since $\ell(HgG_\beta) \leq n-1$, representatives $\beta(HgG_\beta) = t$ and $\beta(Hg) = tb_\beta$ $(b_\beta \in G_\beta)$ have already been chosen; in particular, $\ell(t) \leq n-1$ by (v). Since $\ell(Hg) = n$, we deduce that $b_\beta \neq 1$ and $\ell(tb_\beta) = n$. Define $\alpha(HgG_\alpha) = tb_\beta = \alpha(Hg)$, and whenever $Hg \neq H_i \subseteq HgG_\alpha$, choose $c_\alpha \in G_\alpha$ so that $H_i = Hgc_\alpha$, and put $\alpha(H_i) = tb_\beta c_\alpha$. Clearly, conditions (i)–(v) are satisfied. □

Let us define some key elements of H. Fix an index $\alpha_0 \in A$. For $x \in G_\alpha$ and $H_i \in H\backslash G$, define:

$$y_{i,x} = \alpha(H_i)x\alpha(H_ix)^{-1};$$
$$z_{i,\alpha} = \alpha(H_i)\alpha_0(H_i)^{-1}.$$

It is immediate that $y_{i,x}, z_{i,\alpha} \in H$ all i, x and α. Notice that $z_{1,\alpha} = 1 = z_{i,\alpha_0}$ for all $\alpha \in A$, $i \in I$. If $H_i = Hg$, we often write $y_{Hg,x}$ and $z_{Hg,\alpha}$ for $y_{i,x}$ and $z_{i,\alpha}$. We begin with some simple observations concerning these elements.

Proposition D.3.3 *Retaining the above notation, we have*:

(1) *If* $x_1, x_2 \in G_\alpha$, *then* $y_{i,x_1}y_{j,x_2} = y_{i,x_1x_2}$ *where* $H_ix_1 = H_j$;
(2) *If* $x \in G_\alpha$, $H_i \subseteq HuG_\alpha$ *with* $u = \alpha(HuG_\alpha)$, *then* $y_{i,x} \in uG_\alpha u^{-1} \cap H$;

(3) *If* $h \in uG_\alpha u^{-1} \cap H$ *with* $u = \alpha(HuG_\alpha)$, *then* $h = y_{Hu,x}$ *for some* $x \in G_\alpha$;
(4) *If* $1 \neq u = \alpha(HuG_\alpha)$ *ends with a* β*-syllable, then* $z_{Hu,\alpha} = z_{Hu,\beta}$.

Proof. First we handle (1). Straightforward computation yields

$$y_{i,x_1} y_{j,x_2} = \alpha(H_i)x_1\alpha(H_ix_1)^{-1}\alpha(H_ix_1)x_2\alpha(H_ix_1x_2)^{-1} = y_{i,x_1x_2}.$$

Next we turn to (2). By condition (iii) of a Kurosh system, $\alpha(H_i) = ug$ and $\alpha(H_ix) = ug'$ some $g, g' \in G_\alpha$, whence $y_{i,x} = ugx(ug')^{-1} \in uG_\alpha u^{-1} \cap H$. To prove (3), suppose $h = uxu^{-1}$ with $x \in G_\alpha$. Then $Hu = Hux$ and $\alpha(Hu) = u$ by (i). We conclude $y_{Hu,x} = \alpha(Hu)x\alpha(Hux)^{-1} = uxu^{-1} = h$. For (4) we simply observe $\alpha(Hu) = u = \beta(Hu)$ by (i) and (iv). □

Set $Z = \{z_{i,\alpha} \mid i \in I, \alpha \in A, z_{i,\alpha} \neq 1\}$; note that since $[G : H] < \infty$ and A is finite, the set Z is finite. Let $F = \overline{\langle Z \rangle}$.

From now on we work with a fixed Kurosh system. If $\psi: Z \to K$ is a map, with K a pro-$\mathcal{C}$ group, then we extend ψ to $Z \cup \{1\}$ by setting $\psi(1) = 1$. As usual we set $\Sigma = H\backslash G = H^{abs}\backslash G^{abs}$. We denote by

$$\rho : G \longrightarrow S_\Sigma$$

the representation map (see Section D.1).

Proposition D.3.4 *Given a family* $\mathcal{F} = \{\psi_u: uG_\alpha u^{-1} \cap H \to K\}_{\alpha\in A, u\in D_\alpha}$ *of continuous group homomorphisms and a map* $\psi: Z \to K$ *into a pro-*$\mathcal{C}$ *group* K, *there exists, for each* $\alpha \in A$, *a continuous homomorphism* $\Psi_\alpha: G_\alpha \longrightarrow K \wr \rho(G)$ *defined by* $\Psi_\alpha(x) = (f_x, \rho(x))$ *with*

$$f_x(H_i) = \psi(z_{i,\alpha})^{-1}\psi_u(y_{i,x})\psi(z_{j,\alpha}),$$

where $H_ix = H_j$ *and* $u = \alpha(H_iG_\alpha)$. *If* $\Psi: G \to K \wr \rho(G)$ *denotes the induced homomorphism, then the following diagram commutes*

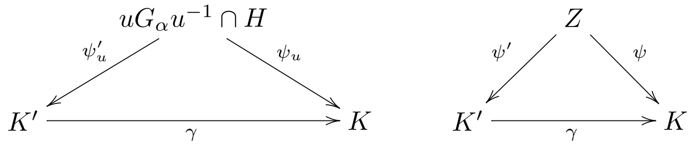
$$\begin{array}{ccc} G & \xrightarrow{\ \Psi\ } & K \wr \rho(G) \\ & \searrow^{\rho} & \downarrow{\scriptstyle\theta} \\ & & \rho(G) \end{array} \qquad (3)$$

where θ *is the projection.*

Moreover, the construction of Ψ *is functorial in the sense that given another family of continuous homomorphisms*

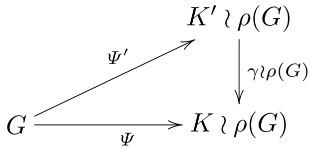
$$\mathcal{F}' = \{\psi'_u: uG_\alpha u^{-1} \cap H \to K'\}_{\alpha\in A, u\in D_\alpha},$$

a map $\psi': Z \longrightarrow K'$ *and a continuous homomorphism* $\gamma: K' \longrightarrow K$ *such that the diagrams*



(4)

commute, then the following diagram commutes



(5)

where Ψ' is the map associated to the family $\mathcal{F}'$.

Proof. The continuity of Ψ_α is clear. We verify that Ψ_α is a homomorphism. Proposition D.3.3(2) implies $y_{i,x} \in uG_\alpha u^{-1} \cap H$ so that Ψ_α makes sense. Let $x_1, x_2 \in G_\alpha$. Clearly, $H_i x_1 G_\alpha = H_i x_2 G_\alpha = H_i x_1 x_2 G_\alpha = H_i G_\alpha$; set $u = \alpha(H_i G_\alpha)$. From

$$(f_{x_1}, \rho(x_1))(f_{x_2}, \rho(x_2)) = (f_{x_1}({}^{\rho(x_1)}f_{x_2}), \rho(x_1 x_2))$$

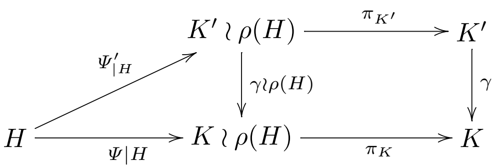
it follows that we just need $f_{x_1}(H_i) f_{x_2}(H_i x_1) = f_{x_1 x_2}(H_i)$. Putting $H_j = H_i x_1$ and $H_k = H_i x_1 x_2$, an application of Proposition D.3.3(1) yields

$$\begin{aligned} f_{x_1}(H_i) f_{x_2}(H_i x_1) &= \psi(z_{i,\alpha})^{-1} \psi_u(y_{i,x_1}) \psi(z_{j,\alpha}) \psi(z_{j,\alpha})^{-1} \psi_u(y_{j,x_2}) \psi(z_{k,\alpha}) \\ &= \psi(z_{i,\alpha})^{-1} \psi_u(y_{i,x_1 x_2}) \psi(z_{k,\alpha}) = f_{x_1 x_2}(H_i), \end{aligned}$$

as required. The Ψ_α induce the desired map Ψ by the universal property of a free product. The commutativity of (3) and (5) are immediate from the definition of Ψ_α and the universal property of a free product. □

From the proposition and Lemma D.1.4, we obtain

Corollary D.3.5 *Let Ψ, Ψ' and γ be as in Proposition* D.3.4*. Then there is a commutative diagram*



(6)

Our next lemma is where we make use of the full strength of the Kurosh system.

Lemma D.3.6 *Let $u = \alpha(Hu)$. Then $f_u(H) = \psi(z_{Hu,\alpha})$.*

Proof. We use induction on the syllable length of u. If $u = 1$, there is nothing to prove as $z_{H,\alpha} = 1$ for all α. So assume $u \neq 1$. The proof divides into two cases.

Case 1. Assume $u \neq \alpha(HuG_\alpha)$. Then (iii) implies we can write $u = vx$ with $v = \alpha(HuG_\alpha)$ and $x \in G_\alpha$. Moreover, $\ell(v) < \ell(u)$ by (ii). Since $\alpha(Hv) = v$ by (i), by induction $f_v(H) = \psi(z_{Hv,\alpha})$. Then we find by Lemma D.1.3

$$\begin{aligned} f_u(H) = f_v(H)f_x(Hv) &= \psi(z_{Hv,\alpha})\psi(z_{Hv,\alpha})^{-1}\psi_v(y_{Hv,x})\psi(z_{Hu,\alpha}) \\ &= \psi_v(y_{Hv,x})\psi(z_{Hu,\alpha}). \end{aligned}$$

But $y_{Hv,x} = \alpha(Hv)x\alpha(Hvx)^{-1} = \alpha(Hv)x\alpha(Hu)^{-1} = vxu^{-1} = 1$, establishing $f_u(H) = \psi(z_{Hu,\alpha})$.

Case 2. Suppose $u = \alpha(HuG_\alpha)$. Since $u \neq 1$, (ii) implies u ends in a syllable β with $\beta \neq \alpha$ and (iv) yields $\beta(Hu) = u$. By (ii) $u \neq \beta(HuG_\beta)$, so Case 1 implies $f_u(H) = \psi(z_{Hu,\beta})$. Proposition D.3.3(4) provides $z_{Hu,\beta} = z_{Hu,\alpha}$, so $f_u(H) = \psi(z_{Hu,\alpha})$. This establishes the lemma. □

An important special case is when $K = H$ and the ψ_u and ψ are the inclusions. Let us denote the induced map in this case by

$$\tilde{\Psi}: G \longrightarrow H \wr \rho(G).$$

Proposition D.3.7 *The map $\tilde{\Psi}: G \longrightarrow H \wr \rho(G)$ is the standard wreath product embedding associated to the transversal T_{α_0}. Consequently, $\pi_H \tilde{\Psi}_{|H}$ is the identity.*

Proof. Writing $\tilde{\Psi}(g) = (F_g, \rho(g))$, if $x \in G_\alpha$ and $H_i x = H_j$, then

$$\begin{aligned} F_x(H_i) = z_{i,\alpha}^{-1} y_{i,x} z_{j,\alpha} &= \alpha_0(H_i)\alpha(H_i)^{-1}[\alpha(H_i)x\alpha(H_j)^{-1}]\alpha(H_j)\alpha_0(H_j)^{-1} \\ &= \alpha_0(H_i)x\alpha_0(H_i x)^{-1}. \end{aligned}$$

Thus $\tilde{\Psi}$ is the standard embedding associated to the transversal T_{α_0}. □

In the proof of the next theorem, we retain all the notation introduced in this section. We restate Theorem D.3.1 in the form that it is needed after the reduction to the case when A is finite.

Theorem D.3.8 *Let G be a free pro-$\mathcal{C}$ product*

$$G = \coprod_{\alpha=1}^{n} G_\alpha.$$

of finitely many pro-$\mathcal{C}$ groups $G_1, \ldots, G_n$. Let H be an open subgroup of G. Fix a Kurosh system $\{D_\alpha, T_\alpha \mid \alpha \in A\}$ for $H \leq_o G$. Then

$$H = \coprod_{\alpha=1}^{n} \left[\coprod_{u \in D_\alpha} \left(uG_\alpha u^{-1} \cap H\right) \right] \amalg F$$

and F is a free pro-$\mathcal{C}$ group with basis Z.

Proof. Let $\{\psi_u: uG_\alpha u^{-1} \cap H \longrightarrow K\}_{\alpha\in A, u\in D_\alpha}$ be a family of continuous group homomorphisms into a pro-$\mathcal{C}$ group K and let $\psi: Z \longrightarrow K$ a map. Let $\Psi: G \longrightarrow K \wr \rho(G)$ be as in Proposition D.3.4. We show $\pi_K\Psi_{|H}$ extends the ψ_u and ψ where $\pi_K = \pi_{K,1}$ is as in Lemma D.1.4. Suppose $u = \alpha(HuG_\alpha)$ and $h \in uG_\alpha u^{-1} \cap H$. By Proposition D.3.3(3), $h = y_{i,x}$ for some $x \in G_\alpha$, where $H_i = Hu$. Setting $H_j = H_i x$, an application of Lemmas D.3.6 and D.1.3 (and the fact $H\alpha(H_i) = H_i$) yields

$$\begin{aligned}
\pi_K\Psi(h) &= f_{y_{i,x}}(H) = f_{\alpha(H_i)x\alpha(H_j)^{-1}}(H)\\
&= f_{\alpha(H_i)}(H) f_x(H_i)\big(f_{\alpha(H_j)}(H_j\alpha(H_j)^{-1})\big)^{-1}\\
&= f_{\alpha(H_i)}(H) f_x(H_i)(f_{\alpha(H_j)}(H))^{-1}\\
&= \psi(z_{i,\alpha})[\psi(z_{i,\alpha})^{-1}\psi_u(y_{i,x})\psi(z_{j,\alpha})]\psi(z_{j,\alpha})^{-1}\\
&= \psi_u(y_{i,x}) = \psi_u(h).
\end{aligned}$$

Similarly, we calculate using Lemmas D.3.6 and D.1.3

$$\begin{aligned}
\pi_K\Psi(z_{i,\alpha}) &= f_{z_{i,\alpha}}(H) = f_{\alpha(H_i)}(H)\big(f_{\alpha_0(H_i)}(H_i\alpha_0(H_i)^{-1})\big)^{-1}\\
&= f_{\alpha(H_i)}(H)(f_{\alpha_0(H_i)}(H))^{-1}\\
&= \psi(z_{i,\alpha})\psi(z_{i,\alpha_0})^{-1} = \psi(z_{i,\alpha})
\end{aligned}$$

since $z_{i,\alpha_0} = 1$.

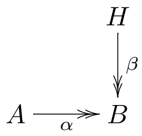
The uniqueness of $\pi_K\Psi_{|H}$ follows from the functoriality of our construction. Namely, in Proposition D.3.4 take $K' = H$ and ψ'_u, ψ' the inclusions (and so $\Psi': G \longrightarrow H \wr \rho(G)$ is $\tilde{\Psi}$ from Proposition D.3.7). Suppose $\gamma: H \longrightarrow K$ is an extension of the ψ_u and ψ. Then (4) commutes and so diagrams (5) and (6) commute. Since $\pi_H\Psi'_{|H} = \pi_H\tilde{\Psi}_{|H}$ is the identity in this case by Proposition D.3.7, we conclude $\gamma = \pi_K\Psi_{|H}$. □

D.4 Subgroups of Projective Groups

In Proposition 7.6.7 projective groups are characterized as those with cohomological dimension at most 1. It follows that a closed subgroup of a projective group is projective. In this section we present a proof of this fact which does not use homology. Instead we deduce this result first for open subgroups using the wreath product embedding of Theorem D.1.2; then a standard argument provides a proof for closed subgroups in general. Under our assumption that $\mathcal{C}$ is extension closed, $\mathcal{C}$-projective groups are just projective groups; so in this section we use only the terminology 'projective' group.

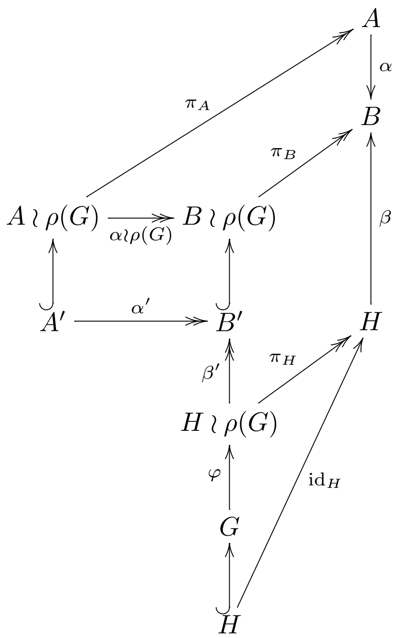
Theorem D.4.1 *Let G be a projective profinite group and let $H \leq_c G$. Then H is projective.*

Proof. We must show (see Lemma 7.6.1) that any embedding problem for H



where A and B are finite, has a weak solution, i.e., there exists a continuous homomorphism $\lambda : H \longrightarrow A$ such that $\alpha\lambda = \beta$.

Case 1. Assume H is open in G. Put $\Sigma = H\backslash G$, and let $\rho : G \longrightarrow S_\Sigma$ be the regular representation. Consider the diagram



where φ is the standard embedding of Theorem D.1.2, B' is the image of the map $G \xrightarrow{\varphi} H \wr \rho(G) \xrightarrow{\beta\wr\rho(G)} B \wr \rho(G)$, $A' = (\alpha \wr \rho(G))^{-1}(B')$, α' is the restriction of $\alpha \wr \rho(G)$ to A', and finally, $\beta' : H \wr \rho(G) \longrightarrow B'$ is the map $x \mapsto (\beta \wr \rho(G))(x)$ $(x \in H \wr \rho(G))$. Since G is projective, there exists a continuous homomorphism $\tilde{\lambda} : G \longrightarrow A'$ such that $\alpha'\tilde{\lambda} = \beta'\varphi$. This diagram commutes thanks to Lemma D.1.4. Define $\lambda : H \longrightarrow A$ to be the composition

$$H \hookrightarrow G \xrightarrow{\tilde{\lambda}} A \wr \rho(G) \xrightarrow{\pi_A} A,$$

(here we are denoting by $\tilde{\lambda}$ again the map $G \xrightarrow{\tilde{\lambda}} B' \hookrightarrow A \wr \rho(G)$). From the commutativity of the diagram, it follows that $\alpha\lambda = \beta$, as required.

Case 2. Assume now that H is any closed subgroup of G. Since $\mathrm{Ker}(\beta)$ is open in H, there exists an open normal subgroup M of G such that $H \cap M \le \mathrm{Ker}(\beta)$. Then $\beta = \beta'\iota$, where $\iota : H \hookrightarrow HM$ is the inclusion and β' is the composition of natural epimorphisms

$$HM \longrightarrow HM/M \cong H/H \cap M \longrightarrow B.$$

Since HM is open we can apply Case 1 to obtain a continuous homomorphism $\lambda' : HM \longrightarrow A$ such that $\alpha\lambda' = \beta'$. Define $\lambda : H \longrightarrow A$ to be $\lambda = \lambda'\iota$; then $\alpha\lambda = \beta$, as needed. □

D.5 Quasifree Profinite Groups

Recall (see Appendix B) that, given a infinite cardinal $\mathfrak{m}$, a pro-$\mathcal{C}$ group G is called $\mathfrak{m}$-quasifree if every split embedding problem

$$\begin{array}{ccc} & & G \\ & & \big\downarrow{\scriptstyle \varphi} \\ A & \xrightarrow[\alpha]{} & B \end{array}$$

with $A, B \in \mathcal{C}$, has exactly $\mathfrak{m}$ different solutions.

Lemma D.5.1 *The minimal number of generators $d(G)$ of an $\mathfrak{m}$-quasifree pro-$\mathcal{C}$ group G is $d(G) = \mathfrak{m}$.*

Proof. By Proposition 2.6.1, $d(G) = w(G)$, the weight of G. So it suffices to prove that $w(G) = \mathfrak{m}$. For any open normal subgroup N of G, the number of continuous epimorphisms $\varphi_N : G \longrightarrow G/N$ with $N = \mathrm{Ker}(\varphi_N)$ is finite. Therefore for any finite group A, the number n_A of open normal subgroups N of G with $G/N \cong A$ equals the number of continuous epimorphisms $G \longrightarrow A$, which in turn equals $\mathfrak{m}$, because G is an $\mathfrak{m}$-quasifree group (just put $B = 1$ in the embedding problem). Now

$$w(G) = \sum_A n_A = \mathfrak{m}\aleph_0 = \mathfrak{m},$$

since the number of isomorphism classes of finite groups is $\aleph_0$. □

Proposition D.5.2 *Let G be an $\mathfrak{m}$-quasifree pro-$\mathcal{C}$ group. Then G contains a free pro-$\mathcal{C}$ group of countable rank.*

Proof. According to Corollary 2.6.6, if H is a pro-$\mathcal{C}$ group that admits a countable set of generators converging to 1, then H contains a countable collection of open normal subgroups

$$H = U_0 > U_1 > \cdots$$

that form a fundamental system of neighborhoods of 1, and so

$$H = \varprojlim_{i \in I} H/U_i \leq \prod_i H/U_i.$$

It follows that H appears as a closed subgroup of the cartesian product of the set of all finite groups in $\mathcal{C}$. In particular the free pro-$\mathcal{C}$ group F of countable rank appears as a closed subgroup of such cartesian product.

Therefore to prove the proposition it is enough to construct an epimorphism $\lambda : G \longrightarrow \prod_{i=0}^{\infty} K_i$, where K_i runs over all finite groups in $\mathcal{C}$, where we assume $K_0 = 1$. To do this we construct inductively compatible epimorphisms

$$\lambda_n : G \longrightarrow \prod_{i=0}^{n} K_i.$$

If λ_{n-1} has been constructed consider the following split embedding problem

$$\begin{array}{ccc} & & G \\ & & \Big\downarrow{\scriptstyle \lambda_{n-1}} \\ \prod_{i=0}^{n} K_i & \xrightarrow{\ \alpha_n\ } & \prod_{i=1}^{n-1} K_i \end{array}$$

where α_n is the natural projection. Since G is quasifree, there exists an epimorphism $\lambda_n : G \longrightarrow \prod_{i=0}^{n} K_i$ such that $\alpha_n \lambda_n = \lambda_{n-1}$ $(n = 1, 2, \ldots)$. The inverse limit of these maps

$$\lambda = \varprojlim {}_n \lambda_n : G \longrightarrow \prod_{i=0}^{\infty} K_i$$

provides the required epimorphism. □

Examples D.5.3

1. Clearly (see also Appendix B) a free profinite group of infinite rank $\mathfrak{m}$ is $\mathfrak{m}$-quasifree.
2. If G is an $\mathfrak{m}$-quasifree group and H is a pro-$\mathcal{C}$ group with $d(H) \leq \mathfrak{m}$, then their free pro-$\mathcal{C}$ product $G \amalg H$ is $\mathfrak{m}$-quasifree.
3. Let $\mathfrak{m}$ be an infinite cardinal. Let $\{G_1, G_2, \ldots\}$ be the collection of all nontrivial finite groups. For each $i = 1, 2, \ldots$ form the free profinite product

   $$A_i = \coprod_{\mathfrak{m}}{}^{r} G_i$$

   of $\mathfrak{m}$ copies of G_i in the sense described in Section D.3. One sees easily that $d(A_i) = \mathfrak{m}$. Define

   $$G = \coprod_i{}^{r} A_i.$$

   Then G is $\mathfrak{m}$-quasifree and it is not projective; in fact G is generated by its torsion elements.

4. (Harbater and Stevenson 2005) Let k be a field and $k((x,t))$ be the fraction field of the power series ring $k[[x,t]]$, where x and t are indeterminates. Let $G = G_{k((x,t))}$ be the absolute Galois group of $k((x,t))$. Denote by $\mathfrak{m}$ the cardinality of $k((x,t))$. Then G is an $\mathfrak{m}$-quasifree profinite group which is not projective.
5. Let F be a free pro-$\mathcal{C}$ group on a countable set of generators

$$x_1, y_1, x_2, y_2, \dots$$

convergent to 1. Observe that the infinite product $[x_1,y_1][x_2,y_2]\cdots$ converges in F and so it defines a unique element r. Define a profinite group G imposing on F the relation $[x_1,y_1][x_2,y_2]\cdots$, i.e., $G = F/(r)$, where (r) denotes the smallest closed normal subgroup of F containing r.

We shall show that G is $\aleph_0$-quasifree. Consider a split embedding problem

$$\begin{array}{ccc} & & G \\ & & \downarrow{\scriptstyle f} \\ A & \xrightarrow{\alpha} & B \end{array}$$

Put K =Ker(α). Let $\theta : B \longrightarrow A$ be a homomorphism such that $\alpha\theta = \mathrm{id}_B$. Then $A = K \rtimes \theta(B)$. Since B is finite, there exists a natural number t such that $f(x_j) = f(y_j) = 1$, for all $j > t$. Let $k_1, \dots, k_n$ be the elements of K.

Next we define an infinite countable set of continuous epimorphism $\{\eta_s : F \longrightarrow A \mid s = 0, 1, 2, \dots\}$. The epimorphism η_s is determined by

$$\eta_s(x_j) = \begin{cases} (\theta f)(x_j), & \text{if } 1 \le j \le t+s; \\ k_i, & \text{if } j = t+s+i, i = 1, \dots, n; \\ 1 & \text{if } j > t+s+n; \end{cases}$$

and

$$\eta_s(y_j) = \begin{cases} (\theta f)(y_j), & \text{if } 1 \le j \le t+s; \\ k_i, & \text{if } j = t+s+i, i = 1, \dots, n; \\ 1 & \text{if } j > t+s+n. \end{cases}$$

Observe that $\eta_s(r) = 1$. Therefore, η_s induces a continuous epimorphism $\lambda_s : G \longrightarrow A$. Moreover $\lambda_s \neq \lambda_{s'}$, if $s \neq s'$, and $\alpha\lambda_s = f$, for all $s = 0, 1, 2, \dots$. Since $d(G) = \aleph_0$, this shows that the above embedding problem has exactly $\aleph_0$ solutions.

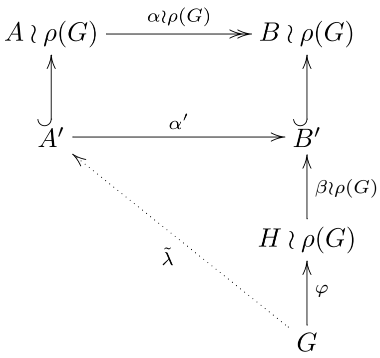
Theorem D.5.4 *Let G be an $\mathfrak{m}$-quasifree pro-$\mathcal{C}$ group, and let H be an open subgroup of G. Then H is $\mathfrak{m}$-quasifree.*

Proof. Given $A, B \in \mathcal{C}$, a proper split epimorphism $\alpha: A \longrightarrow B$ and a continuous epimorphism $\beta: H \longrightarrow B$, we need to prove the existence of exactly $\mathfrak{m}$ continuous epimorphisms $\lambda: H \longrightarrow A$ such that $\alpha\lambda = \beta$.

Set $\Sigma = H\backslash G$ and let $\rho: G \longrightarrow S_\Sigma$ be the corresponding permutation representation as in Section D.1. Consider the standard embedding

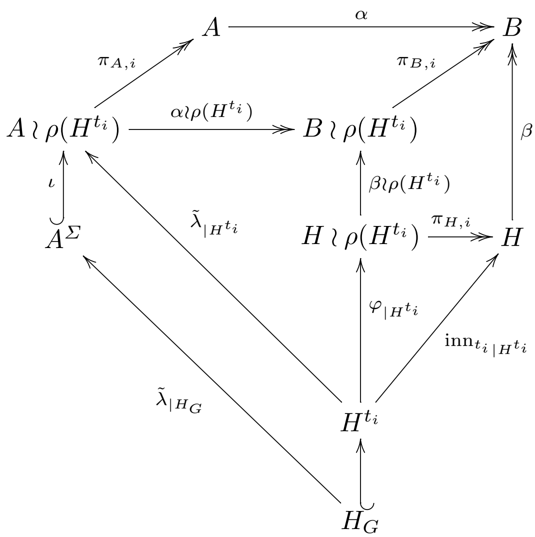
$$\varphi: G \longrightarrow H \wr \rho(G)$$

constructed in Theorem D.1.2. Note that $\alpha \wr \rho(G): A \wr \rho(G) \longrightarrow B \wr \rho(G)$ is a split proper epimorphism by Proposition D.1.1; observe also that $A \wr \rho(G)$ and $B \wr \rho(G)$ are finite groups in $\mathcal{C}$, as $\mathcal{C}$ is extension closed. Let $B' = (\beta \wr \rho(G))\varphi(G)$ and $A' = (\alpha \wr \rho(G))^{-1}(B')$. Then $A', B' \in \mathcal{C}$, and the restriction $\alpha': A' \longrightarrow B'$ of $\alpha \wr \rho(G)$ to A' is a split proper epimorphism.



Since G is $\mathfrak{m}$-quasifree, there exists a continuous epimorphism $\tilde{\lambda}: G \longrightarrow A'$ such that $\alpha'\tilde{\lambda} = (\beta \wr \rho(G))\varphi$. Then, for each $g \in G$, $\tilde{\lambda}(g) = (\tilde{f}_g, \rho(g))$, for some $\tilde{f}_g \in A^\Sigma$.

Let $T = \{t_1 = 1, t_2, \dots, t_k\}$ be a right transversal of H in G. For $i = 1, \dots, k$, define $\lambda_i: H^{t_i} \longrightarrow A$ to be $\lambda_i = \pi_{A,i}\tilde{\lambda}_{|H^{t_i}}$, i.e., $\lambda_i(x) = \tilde{f}_x(Ht_i)$, for $x \in H^{t_i}$. According to Lemma D.1.4, the diagram



commutes. Thus $\beta \circ \mathrm{inn}_{t_i|H^{t_i}} = \alpha\lambda_i$.

We claim that λ_i is surjective. Let $a \in A$ and let $b = \alpha(a)$. Since β is surjective, the commutativity of the above diagram ensures that there exists $(f, \rho(x)) \in (B \wr \rho(H^{t_i})) \cap B'$, where $x \in H^{t_i}$, with $f(Ht_i) = b$. Choose $f'\colon \Sigma \to A$ to be any function so that $f'(Ht_i) = a$ and $\alpha f' = f$; then $(f', \rho(x)) \in A'$. Therefore, $\pi_{A,i}$ takes $A' \cap (A \wr \rho(H^{t_i}))$ onto A. Because $\mathrm{Ker}\tilde{\lambda} \leq \mathrm{Ker}\rho = H_G \leq H^{t_i}$, it follows that $\tilde{\lambda}(g) \in A \wr \rho(H^{t_i})$ implies $g \in H^{t_i}$. We deduce that $\tilde{\lambda}_{|H^{t_i}}\colon H^{t_i} \to A' \cap (A \wr \rho(H^{t_i}))$ is an epimorphism, and hence so is λ_i, proving the claim.

Since G is quasifree, the total number of epimorphisms $\tilde{\lambda}\colon G \longrightarrow A'$ such that $\alpha'\tilde{\lambda} = (\beta \wr \rho(G))\varphi$ is $\mathfrak{m}$. Since $H_G = \bigcap_{i=1}^k H^{t_i}$ has finite index in G, these $\tilde{\lambda}$ restrict to $\mathfrak{m}$ different homomorphisms

$$\tilde{\lambda}_{|H_G}\colon H_G \longrightarrow A \wr \rho(H_G) = A^{\Sigma}.$$

Recalling from Lemma D.1.4 that the $\pi_{A,i}\colon A^{\Sigma} \to A$ $(i = 1, \ldots, k)$ are the direct product projections, we conclude that $\tilde{\lambda}_{|H_G}$ is determined by the maps $\pi_{A,i}\tilde{\lambda}_{|H_G} = \lambda_{i|H_G}$, $i = 1, \ldots, k$. It follows that there exists some $j \in \{1, \ldots, k\}$, such that the number of different maps $\lambda_{j|H_G}$ constructed in this manner is precisely $\mathfrak{m}$.

For each of these λ_j, define $\lambda = \lambda_j \circ \mathrm{inn}_{t_j^{-1}|H}$. Then, since H_G has finite index in H, we have constructed $\mathfrak{m}$ different epimorphisms $\lambda\colon H \longrightarrow A$ such that $\alpha\lambda = \beta$. Finally, observe that there cannot be more such λ since the minimal number $d(H)$ of generators of H converging to 1 is $\mathfrak{m}$ and A is finite. This completes the proof. □

D.6 Notes, Comments and Further Reading

Most of this appendix is based on Ribes and Steinberg [2010], where also conceptually simple proofs for the Nielsen-Schreier Theorem and the Kurosh theorem for abstract groups are explicitly given using wreath products. The proof that we present here of Theorem D.4.1 is due to Cossey, Kegel and Kovács [1980]; the result was known earlier: it is clear from the cohomological characterization of projective groups given in Proposition 7.6.7 (cf. Gruenberg [1967]). The results in D.5 appeared first in Ribes, Stevenson and Zalesskii [2007]; the proof of Theorem D.5.4 that we present here is from Ribes and Steinberg [2010]. In Bary-Soroker, Haran and Harbater [2010] a concept similar to $\mathfrak{m}$-quasifree is introduced and several subgroup theorems are proved using also wreath products. See also Ershov [1998]. For uses of wreath products in the context of profinite semigroups see Steinberg [2009] and Rhodes and Steinberg [2008].

Bibliography

Abért, M., Hededűs, P.: On the number of generators needed for free profinite products of finite groups. Isr. J. Math. **162**, 81–92 (2007)

Alperin, J.: Sylow intersections and fusion. J. Algebra **6**, 222–241 (1967)

Anderson, M.P.: Exactness properties of profinite completions of functors. Topology **13**, 229–239 (1974)

Anderson, M.P.: Subgroups of finite index in profinite groups. Pac. J. Math. **62**, 19–28 (1976)

Andreadakis, S.: On the automorphisms of free groups and free nilpotent groups. Proc. Lond. Math. Soc. **15**(3), 239–268 (1965)

Appelgate, H., Onishi, H.: Coincident pairs of continuous sections in profinite groups. Proc. Am. Math. Soc. **63**, 217–220 (1977)

Barnea, Y., Larsen, M.: A non-abelian free pro-p group is not linear over a local field. J. Algebra **214**, 338–341 (1999)

Bary-Soroker, L.: Diamond theorem for a finitely generated free profinite group. Math. Ann. **336**(4), 949–961 (2006)

Bary-Soroker, L., Haran, D., Harbater, D.: Permanence criteria for semi-free profinite groups. Math. Ann. (2010, to appear)

Bass, H., Lubotzky, A.: Nonarithmetic superrigid groups: counterexamples to Platonov's conjecture. Ann. Math. (2) **151**(3), 1151–1173 (2000)

Bass, H., Lazard, M., Serre, J-P.: Sous-groupes d'indice fini dans $\mathrm{SL}_n(\mathbf{Z})$. Bull. Am. Math. Soc. **70**, 385–392 (1964)

Baumslag, G.: On residual finiteness of generalized products of nilpotent groups. Trans. Am. Math. Soc. **106**, 193–209 (1963)

Baumslag, B., Pride, S.J.: Groups with two more generators than relators. J. Lond. Math. Soc. **17**(2), 425–426 (1978)

Bieri, R.: Homological Dimension of Discrete Groups. Queen Mary College Math. Notes, London (1976)

Binz, E., Neukirch, J., Wenzel, G.H.: A subgroup theorem for free products of profinite groups. J. Algebra **19**, 104–109 (1971)

Bolker, E.D.: Inverse limits of solvable groups. Proc. Am. Math. Soc. **14**, 147–152 (1963)

Borovik, A.V., Pyber, L., Shalev, A.: Maximal subgroups in finite and profinite groups. Trans. Am. Math. Soc. **348**, 3745–3761 (1996)

Bourbaki, N.: Algèbre ch. 5. Hermann, Paris (1967)

Bourbaki, N.: General Topology. Springer, Berlin (1989)

Brauer, R.: Über die Konstruktion des Schiefkörper, die von endlichen Rang in bezug auf gegebenes Zentrum sind. J. Reine Angew. Math. **168**, 44–64 (1932)

Brauer, W.: Über gewisse Verbände von Untergruppen pro-enlicher Gruppen. Math. Z. **109**, 177–190 (1969)

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4, © Springer-Verlag Berlin Heidelberg 2010

Bridson, M.R., Grunewald, F.J.: Grothendieck's problems concerning profinite completions and representations of groups. Ann. Math. **160**, 359–373 (2004)

Brown, K.S.: Cohomology of Groups. Springer, Berlin (1982)

Brumer, A.: Pseudocompact algebras, profinite groups and class formations. J. Algebra **4**, 442–470 (1966)

Camina, R.: Subgroups of the Nottingham group. J. Algebra **196**, 101–113 (1997)

Cartan, H., Eilenberg, S.: Homological Algebra. Princeton Univ. Press, Princeton (1956)

Chatzidakis, Z.A.: Some remarks on profinite HNN extensions. Isr. J. Math. **85**, 11–18 (1994)

Chatzidakis, Z.A.: Model theory of profinite groups having the Iwasawa property. Ill. J. Math. **42**, 70–96 (1998)

Chatzidakis, Z.A.: Torsion in pro-p completions of torsion free groups. J. Group Theory **2**, 65–68 (1999)

Chatzidakis, Z.A., Pappas, P.: Von Neumann regular rings not representable as rings of continuous functions. Algebra Univers. **29**, 332–337 (1992)

Cherlin, G., van den Dries, L., Macintyre, A.: The elementary theory of regularly closed fields. Manuscript (1984)

Cossey, J., Kegel, G.H., Kovács, L.G.: Maximal Frattini extensions. Arch. Math. **35**, 210–217 (1980)

Crawley-Boevey, W.W., Kropholler, P.H., Linnell, P.A.: Torsion-free soluble groups, completions, and the zero divisor conjecture. J. Pure Appl. Algebra **54**, 181–196 (1988)

Demushkin, S.: The group of a maximal p-extension of a local field. Dokl. Akad. Nauk SSSR **128**, 657–660 (1959) (Russian)

Demushkin, S.: On the 2-extensions of a local field. Sib. Mat. Zh. **4**, 951–955 (1963) (Russian)

Deschamps, B., Leloup, G.: La structure profinie du groupe des unités d'un anneau de séries entières à coefficients dans un anneau fini. J. Algebra **295**, 81–93 (2006)

Detomi, E., Lucchini, A.: Non-prosoluble profinite groups with a rational probabilistic zeta function. J. Group Theory **10**, 453–466 (2007)

Diaz-Barriga, A., López, L.Y.: Sumas activas de grupos pro-$\mathcal{C}$. An. Inst. Mat. Univ. Nac. Autón. Méx. **19**, 21–39 (1979)

Dicks, W., Formanek, E.: The rank three case of the Hanna Neumann conjecture, Centre Rec. Mat., Univ. Auto. Barcelona, preprint (1999)

Dikranjan, D.N., Prodanov, I.R., Stoyanov, L.N.: Topological Groups. Dekker, New York (1990)

Dixon, J., Formanek, E., Poland, J., Ribes, L.: Profinite completions and isomorphic finite quotients. J. Pure Appl. Algebra **23**, 227–231 (1982)

Dixon, J.D., du Sautoy, M.P.F., Mann, A., Segal, D.: Analytic Pro-p Groups, 2nd edn. Cambridge Studies in Advanced Math., vol. 61. Cambridge Univ. Press, Cambridge (1999). The first edition was published in 1991

Doerk, K., Hawkes, T.: Finite Soluble Groups. de Gruyter, Berlin (1992)

Douady, A.: Cohomologie des groupes compacts totalement discontinus. Séminaire Bourbaki, 1959–1960, Exposé 189 (1960)

Douady, A.: Détermination d'un groupe de Galois. C. R. Acad. Sc. Paris **258**, 5305–5308 (1964)

Dummit, D., Labute, J.: On a new characterization of Demuskin groups. Invent. Math. **73**, 413–418 (1983)

du Sautoy, M.P.F.: Finitely generated groups, p-adic analytic groups and Poincaré series. Ann. Math. (2) **137**, 639–670 (1993)

du Sautoy, M., Grunewald, F.: Zeta functions of groups: zeros and friendly ghosts. Am. J. Math. **124**, 1–48 (2002)

du Sautoy, M.P.F., Segal, D., Shalev, A. (eds.): New Horizons in Pro-p Groups. Birkhäuser, Boston (2000)

Efrat, I.: Free pro-p product decompositions of Galois groups. Math. Z. **225**, 245–261 (1997)

Efrat, I., Haran, D.: On Galois groups over Pythagorean and semi-real closed fields. Isr. J. Math. **85**, 57–78 (1994)

Eilenberg, S., Steenrod, N.: Foundations of Algebraic Topology. Princeton Univ. Press, Princeton (1952)

Ershov, Yu.: Profinite groups. Algebra Log. **19**, 552–565 (1980). English transl.: Algebra Log. **19**, 357–366

Ershov, Yu.L.: Free products of absolute Galois groups. Dokl. Math. **56**, 915–917 (1997)

Ershov, Yu.L.: On a theorem of Kurosh. Algebra Log. **37**, 381–393 (1998). English trans.: Algebra Log. **37**, 215–222

Ershov, Yu., Fried, M.: Frattini covers and projective groups without the extension property. Math. Ann. **253**, 322–339 (1980)

Evans, M.J.: Torsion in pro-finite completions of torsion-free groups. J. Pure Appl. Algebra **65**, 101–104 (1990)

Fernández-Alcober, G.A., González-Sánchez, J., Jaikin-Zapirain, A.: Omega subgroups of pro-p groups. Isr. J. Math. **166**, 393–412 (2008)

Fried, M.D., Jarden, M.: Field Arithmetic, 3rd edn. Springer, Berlin (2008). Revised by Jarden

Fuchs, L.: Infinite Abelian Groups, vol. I. Academic Press, New York (1970)

Fujiwara, K.: The second bounded cohomology of an amalgamated free product of groups. Trans. Am. Math. Soc. **352**, 1113–1129 (2000)

Gaschütz, W.: Zur Erweiterungstheorie endlicher Gruppen. J. Math. **190**, 93–107 (1952)

Gaschütz, W.: Zu einem von B.H. Neuman gestellten Problem. Math. Nachr. **14**, 249–252 (1956)

Gildenhuys, D.: On pro-p-groups with a single defining relator. Invent. Math. **5**, 357–366 (1968)

Gildenhuys, D., Lim, C.K.: Free pro-$\mathcal{C}$ groups. Math. Z. **125**, 233–254 (1972)

Gildenhuys, D., Ribes, L.: A Kurosh subgroup theorem for free products of pro-$\mathcal{C}$-groups. Trans. Am. Math. Soc. **186**, 309–329 (1973)

Gildenhuys, D., Ribes, L.: On the cohomology of certain topological colimits of pro-$\mathcal{C}$-groups. J. Algebra **29**, 172–197 (1974)

Gildenhuys, D., Herfort, W.N., Ribes, L.: Profinite Frobenius groups. Arch. Math. **33**, 518–528 (1979)

Gildenhuys, D., Ivanov, S., Kharlampovich, O.: On a family of one-relator pro-p-groups. Proc. R. Soc. Edinb. **124A**, 1199–1207 (1994)

Gilotti, A.L., Ribes, L., Serena, L.: Fusion in profinite groups. Ann. Mat. Pura Appl. **CLXXVII**, 349–362 (1999)

Goldman, O., Sah, C.-H.: On a special class of locally compact rings. J. Algebra **4**, 71–95 (1966)

Goldstein, D., Guralnick, R.M.: The direct product theorem for profinite groups. J. Group Theory **9**, 317–322 (2006)

Golod, E.S., Shafarevich, I.R.: On class field towers. Izv. Akad. Nauk SSSR **28**, 261–272 (1964). English transl.: Am. Math. Soc. Transl. (2) **48**, 91–102 (1964)

Grigorchuk, R.I.: On the Burnside problem for periodic groups. Funct. Anal. Appl. **14**, 53–54 (1980)

Grigorchuk, R.I.: Bounded cohomology of group constructions. Math. Notes **59**, 392–394 (1996)

Grigorchuk, R.I., Herfort, W.N., Zalesskii, P.A.: The profinite completion of certain torsion p-groups. In: Algebra, Moscow, 1998, pp. 113–123. de Gruyter, Berlin (2000)

Grothendieck, A.: Sur quelque points d'algèbre homologique. Tôhoku Math. J. **9**, 119–221 (1957)

Grothendieck, A.: Representations lineaires et compactification profinie des groupes discrets. Manuscr. Math. **2**, 375–396 (1970)

Gruenberg, K.W.: Projective profinite groups. J. Lond. Math. Soc. **42**, 155–165 (1967)

Gruenberg, K.W.: Cohomological Topics in Group Theory. Lect. Notes Math., vol. 143. Springer, Berlin (1970)

Grunewald, F.J., Pickel, P.-F., Segal, D.: Polycyclic groups with isomorphic finite quotients. Ann. Math. (2) **111**, 155–195 (1980)

Grunewald, F., Jaikin-Zapirain, A., Pinto, A.G.S., Zalesskii, P.A.: Normal subgroups of profinite groups of non-negative deficiency. Preprint (2008)

Gupta, N., Sidki, S.: On the Burnside problem for periodic groups. Math. Z. **182**, 385–388 (1983)

Guralnick, R.M., Haran, D.: Frobenius subgroups of free profinite products. arXiv:1001.3599 (2010)

Guralnick, R., Kantor, W.M., Kassabov, M., Lubotzky, A.: Presentations of finite simple groups: profinite and cohomological approaches. Groups, Geom. Dyn. **1**, 469–523 (2007)

Hall, M., Jr.: Coset representations in free groups. Trans. Am. Math. Soc. **67**, 421–432 (1949)

Hall, M., Jr.: A topology for free groups and related groups. Ann. Math. (2) **52**, 127–139 (1950)

Hall, P.: Some sufficient condition for a group to be nilpotent. Ill. J. Math. **2**, 787–801 (1958)

Hall, M., Jr.: The Theory of Groups. Macmillan Co., New York (1959)

Haran, D.: A proof of Serre's theorem. J. Indian Math. Soc. **55**, 213–234 (1990)

Haran, D.: Free subgroups of free profinite groups. J. Group Theory **2**, 307–317 (1999)

Haran, D., Lubotzky, A.: Embedding covers and the theory of Frobenius fields. Isr. J. Math. **41**, 181–202 (1983)

Haran, D., Lubotzky, A.: Maximal abelian subgroups of free profinite groups. Math. Proc. Camb. Philos. Soc. **97**, 51–55 (1985)

Harbater, D.: Fundamental groups and embedding problems in characteristic p. Contemp. Math., Am. Math. Soc. **186**, 353–369 (1995)

Harbater, D., Stevenson, K.F.: Local Galois theory in dimension two. Adv. Math. **198**(2), 623–653 (2005)

Hartley, B.: Subgroups of finite index in profinite groups. Math. Z. **168**, 71–76 (1979)

Hensel, K.: Theorie der Algebraischen Zahlen. Teuber, Leipzig (1908)

Herfort, W.N.: Compact torsion groups and finite exponent. Arch. Math. **33**, 404–410 (1980)

Herfort, W.N.: An Arithmetic property of finite groups. Manuscr. Math. **37**, 11–17 (1982)

Herfort, W.N., Ribenboim, P.: Localization of profinite groups. Arch. Math. **42**, 1–15 (1984)

Herfort, W.N., Ribes, L.: Torsion elements and centralizers in free products of profinite groups. J. Reine Angew. Math. **358**, 155–161 (1985)

Herfort, W.N., Ribes, L.: Solvable subgroups of free products of profinite groups. In: Proc. 1987 Singapore Group Theory Conference, pp. 391–403. de Gruyter, Berlin (1989a)

Herfort, W.N., Ribes, L.: Frobenius subgroups of free products of prosolvable groups. Monatsh. Math. **108**, 165–182 (1989b)

Hewitt, E., Ross, K.A.: Abstract Harmonic Analysis I. Springer, Berlin (1963)

Hewitt, E., Ross, K.A.: Abstract Harmonic Analysis II. Springer, Berlin (1970)

Higman, G.: A finitely generated infinite simple group. J. Lond. Math. Soc. **26**, 61–64 (1951)

Hillman, J., Schmidt, A.: Pro-p groups of positive deficiency. Bull. LMS **40**, 1065–1069 (2008)

Hochschild, G.P., Serre, J-P.: Cohomology of group extensions. Trans. Am. Math. Soc. **74**, 110–134 (1953)

Hofmann, K.H., Morris, S.A.: The Structure of Compact Groups, 2nd edn. de Gruyter, Berlin (2006)

Howson, A.G.: On the intersection of finitely generated free groups. J. Lond. Math. Soc. **29**, 428–434 (1954)

Huppert, B.: Normalteiler und maximale Untergruppen endlicher Gruppen. Math. Z. **60**, 409–434 (1954)

Huppert, B.: Endliche Gruppen I. Springer, Berlin (1967)

Ikeda, M.: Completeness of the absolute Galois group of the rational number field. J. Reine Angew. Math. **291**, 1–22 (1977)

Iwasawa, I.: On solvable extensions of algebraic number fields. Ann. Math. **58**, 548–572 (1953)

Jaikin-Zapirain, A.: On linear just infinite pro-p groups. J. Algebra **255**(2), 392–404 (2002)

Jaikin-Zapirain, A.: On the verbal width of finitely generated pro-p groups. Rev. Mat. Iberoam. **24**, 617–630 (2008)

Jarden, M.: Normal automorphisms of free profinite groups. J. Algebra **62**, 118–123 (1980)

Jarden, M.: On free profinite groups of uncountable rank. Contemp. Math., Am. Math. Soc. **186**, 371–383 (1995)

Jarden, M., Lubotzky, A.: Hilbertian fields and free profinite groups. J. Lond. Math. Soc. **46**, 205–227 (1992)

Jarden, M., Ritter, J.: Normal automorphisms of absolute Galois groups of $\mathfrak{p}$-adic fields. Duke Math. J. **47**, 47–56 (1980)

Johnson, D.L.: The group of formal power series under substitution. J. Aust. Math. Soc. **45**, 296–302 (1988)
Joly, J.R.: Groupes procycliques. C. R. Acad. Sc. Paris **261**, 13–15 (1965)
Kargapolov, M.I., Merzljakov, Ju.I.: Fundamentals of the Theory of Groups. Springer, Berlin (1979)
Kassabov, M., Nikolov, N.: Cartesian products as profinite completions. Int. Math. Res. Not. Art. ID 72947, p. 17 (2006)
Kharlampovich, O., Myasnikov, A.: Implicit function theorem over free groups. J. Algebra **290**, 1–203 (2005)
Kilsch, D.: Fitting subgroups of profinite completions of soluble minimax groups. J. Algebra **101**, 120–126 (1986)
Klaas, G., Leedham-Green, C.R., Plesken, W.: Linear Pro-p-groups of Finite Width. Lect. Notes Math., vol. 1674. Springer, Berlin (1997)
Koch, H.: Galoissche Theorie der p-Erweiterungen. VEB, Berlin (1970)
Kochloukova, D., Pinto, A.G.S.: Centre-by-metabelian pro-p groups of type FP_m. Math. Proc. Camb. Philos. Soc. **145**, 305–309 (2008)
Kochloukova, D.H., Zalesskii, P.A.: On pro-p analogues of limit groups via extensions of centralizers. Math. Z. (2010, to appear)
Koenigsmann, J.: Relatively projective groups as absolute Galois groups. Isr. J. Math. **127**, 93–129 (2002)
Koenigsmann, J.: Products of absolute Galois groups. Int. Math. Res. Not. **24**, 1465–1486 (2005)
Kovács, L.G., Sim, H.-S.: Generating finite soluble groups. Indag. Math. **2**(1991), 229–232 (1991)
Kropholler, P.H., Wilson, J.S.: Torsion in profinite completions. J. Pure Appl. Algebra **88**, 143–154 (1993)
Krull, W.: Galoissche Theorie der unendlichen algebraischen Erweiterungen. Math. Ann. **100**, 687–698 (1928)
Labute, J.P.: Classification of Demushkin groups. Can. J. Math. **19**, 106–132 (1966a)
Labute, J.P.: Demushkin groups of rank $\aleph_0$. Bull. Soc. Math. Fr. **94**, 211–244 (1966b)
Labute, J.P.: Algèbres de Lie et pro-p groupes definis par une seule relation. Invent. Math. **4**, 142–158 (1967)
Lang, S.: Rapport sur la Cohomologie des Groupes. Benjamin, New York (1966)
Lazard, M.: Sur les groupes nilpotentes et les anneaux de Lie. Ann. Sci. E.N.S. **71**, 101–190 (1954)
Lazard, M.: Groupes analytiques p-adiques. Publ. Math. I.H.E.S. **26**, 389–603 (1965)
Leptin, H.: Ein Darstellungssatz für kompakte, total unzusammenhängende Gruppen. Arch. Math. **6**, 371–373 (1955)
Lim, C.-K.: Pro-nilpotent groups. Nanta Math. **VI**, 58–59 (1973a)
Lim, C.-K.: A corollary to Lazard's theorem on pro-p-groups. J. Lond. Math. Soc. (2) **6**, 570 (1973b)
Linnell, P.A., Warhurst, D.: Bounding the number of generators of a polycyclic group. Arch. Math. **37**, 7–17 (1981)
Lubotzky, A.: Tannaka duality for discrete groups. Am. J. Math. **102**, 663–689 (1980)

Lubotzky, A.: Combinatorial group theory for pro-p groups. J. Pure Appl. Algebra **25**, 311–325 (1982)
Lubotzky, A.: Group presentation, p-adic analytic groups and lattices in $SL_2(\mathbf{C})$. Ann. Math. **118**, 115–130 (1983)
Lubotzky, A.: Torsion in profinite completions of torsion-free groups. Q. J. Math. Oxf. **44**, 327–332 (1993)
Lubotzky, A.: Subgroup growth and congruence subgroups. Invent. Math. **119**, 267–295 (1995)
Lubotzky, A.: Pro-finite presentations. J. Algebra **242**, 672–690 (2001)
Lubotzky, A., Mann, A.: Residually finite groups of finite rank. Math. Proc. Camb. Philos. Soc. **106**, 385–388 (1989)
Lubotzky, A., Segal, D.: Subgroup Growth. Birkhäuser, Basel (2003)
Lubotzky, A., van den Dries, L.: Subgroups of free profinite groups and large subfields of $\tilde{\mathbf{Q}}$. Isr. J. Math. **39**, 25–45 (1981)
Lubotzky, A., Wilson, J.S.: An embedding theorem for profinite groups. Arch. Math. **42**, 397–399 (1984)
Lucchini, A.: Generating the augmentation ideal. Red. Sem. Mat. Univ. Padova **88**, 145–149 (1992)
Lucchini, A.: On the minimal number of generators of free profinite products of profinite groups. J. Group Theory **4**, 53–58 (2001a)
Lucchini, A.: On the number of generators of finite images of free products of finite groups. J. Algebra **245**, 552–561 (2001b)
Lucchini, A., Menegazzo, F., Morigi, M.: On the probability of generating prosoluble groups. Isr. J. Math. **155**, 93–115 (2006)
Lyndon, R.C.: Cohomology theory of groups with a single defining relation. Ann. Math. **52**, 650–665 (1950)
Lyndon, R.C., Schupp, P.E.: Combinatorial Group Theory. Springer, Berlin (1977)
Mac Lane, S.: Homology. Springer, Berlin (1963)
Mac Lane, S.: Categories for the Working Mathematician. Springer, Berlin (1971)
Magnus, W., Karras, A., Solitar, D.: Combinatorial Group Theory. Interscience, New York (1966)
Mann, A., Segal, D.: Uniform finiteness conditions in residually finite groups. Proc. Lond. Math. Soc. (3) **61**, 529–545 (1990)
Martínez, C.: On Power subgroups of profinite groups. Trans. Am. Math. Soc. **345**, 865–869 (1994)
Martínez, C.: Power subgroups of pro-(finite soluble) groups. Bull. Lond. Math. Soc. **28**, 481–483 (1996)
Martínez, C., Zel'manov, E.: Products of powers in finite simple groups. Isr. J. Math. **96**, 469–479 (1996)
Matzat, B.H.: Konstruktive Galoistheorie. Springer, Berlin (1987)
McCleary, J.: User's Guide to Spectral Sequences. Publish or Perish, Delaware (1985)
McMullen, J.R.: Compact torsion groups. In: Proc. 2nd Int. Conf. Theory of Groups 1973. Lect. Notes Math., vol. 372, pp. 453–462. Springer, Berlin (1974)
McMullen, J.R.: The profinite completion of certain residually finite p-groups. Monatsh. Math. **99**, 311–314 (1985)
Mel'nikov, O.V.: The congruence kernel of the group $SL_2(\mathbf{Z})$. Dokl. Akad. Nauk **228**, 1034–1036 (1976). English transl.: Sov. Math. Dokl. **17**, 867–870

Mel'nikov, O.V.: Normal subgroups of free profinite groups. Izv. Akad. Nauk **42**, 3–25 (1978). English transl.: Math. USSR Izv. **12**, 1–20

Mel'nikov, O.V.: Projective limits of free profinite groups. Dokl. Akad. Nauk BSSR **24**, 968–970 (1980)

Mel'nikov, O.V.: Characteristic subgroups and automorphisms of free profinite groups. Mat. Zametki **31**, 339–349 (1982)

Mel'nikov, O.V.: Structure of free profinite groups and products. Dissertation, Institute of Mathematics, Akad. Nauk BSSR, Minsk (1988)

Mel'nikov, O.V.: On free products of absolute Galois groups. Sib. Mat. Zh. **40**, 113–118 (1997). English transl.: Sib. Math. J. **40**, 95–99 (1999)

Mennicke, J.L.: Finite factor groups of the unimodular group. Ann. Math. (2) **81**, 31–37 (1965)

Morris, S.A.: Pontryagin Duality and the Structure of Locally Compact Abelian Groups. London Math. Soc. Lect. Notes, vol. 29. Cambridge Univ. Press, Cambridge (1977)

Myasnikov, A.G., Remeslennikov, V.N.: Recursive p-adic numbers and elementary theories of finitely generated pro-p-groups. Izv. Akad. Nauk SSSR. **51** (1987). English transl.: Math. USSR Izv. **30**, 577–597 (1988)

Neukirch, J.: Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper. Invent. Math. **6**, 296–314 (1969)

Neukirch, J.: Freie Produkte pro-enlicher Gruppen und ihre Kohomologie. Arch. Math. **22**, 337–357 (1971)

Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields, 2nd edn. Springer, Berlin (2008)

Nikolov, N., Segal, D.: On finitely generated profinite groups, I: strong completeness and uniform bounds. Ann. Math. **165**, 171–238 (2007a)

Nikolov, N., Segal, D.: On finitely generated profinite groups, II: products in quasisimple groups. Ann. Math. **165**, 239–273 (2007b)

Noskov, G.A.: Number of generators of a group. Mat. Zametki **33**, 489–498 (1983)

Oltikar, B.C., Ribes, L.: On prosupersolvable groups. Pac. J. Math. **77**, 183–188 (1978)

Peterson, H.L.: Discontinuous characters and subgroups of finite index. Pac. J. Math. **44**, 683–691 (1973)

Pickel, P.F.: Fitting subgroups and profinite completions of polycyclic groups. J. Algebra **42**, 41–45 (1976)

Platonov, V.P.: Periodic and compact subgroups of topological groups. Sib. Math. **7**, 854–877 (1966)

Platonov, V.P., Rapinchuk, A.S.: Algebraic Groups and Number Theory. Academic Press, New York (1993)

Platonov, V.P., Tavgen, O.P.: On Grothendieck's problem on profinite completions of groups. Sov. Math. Dokl. **33**, 822–825 (1986)

Platonov, V.P., Tavgen, O.P.: Grothendieck's problem on profinite completions and representations of groups. K-Theory **4**, 89–101 (1990)

Pletch, A.: Profinite duality groups I. J. Pure Appl. Algebra **16**, 55–74 (1980a)

Pletch, A.: Profinite duality groups II. J. Pure Appl. Algebra **16**, 285–297 (1980b)

Pletch, A.: Strong completeness in profinite groups. Pac. J. Math. **97**, 203–208 (1981)

Pletch, A.: Local freeness of profinite groups. Can. Math. Bull. **25**, 441–446 (1982)

Poitou, G.: Cohomologie Galoisienne des Modules Finis. Dunod, Paris (1967)

Pop, F.: Classically projective groups and pseudo classically closed fields. Preprint, Math. Institut, Heidelberg (1990)

Pop, F.: Embedding problems over large fields. Ann. Math. **144**, 1–34 (1996)

Pyber, L.: Groups of intermediate subgroup growth and a problem of Grothendieck. Duke Math. J. **121**(1), 169–188 (2004)

Rapinchuk, A.S.: On SS-rigid groups and A. Weil's criterion for local rigidity I. Manuscr. Math. **97**, 529–543 (1998)

Rapinchuk, A.S.: The congruence subgroup problem. Contemp. Math. **243**, 175–188 (1999)

Remeslennikov, V.N.: Embedding theorems for profinite groups. Izv. Akad. Nauk SSSR **43** (1979). English transl.: Math. USSR Izv. **14**, 367–382 (1980)

Rhemtulla, A.H.: Commutators of certain finitely generated soluble groups. Can. J. Math. **21**, 1160–1164 (1969)

Rhodes, J., Steinberg, B.: The $\mathfrak{q}$-theory of Finite Semigroups. Springer, Berlin (2008)

Ribes, L.: Profinite Groups and Galois Cohomology. Queens Papers Pure Appl. Math., vol. 24. Kingston, Canada (1970). Reprinted with a list of errata in 1999

Ribes, L.: On amalgamated products of profinite groups. Math. Z. **123**, 357–364 (1971)

Ribes, L.: Amalgamated product of profinite groups: counterexamples. Proc. Am. Math. Soc. **37**, 413–416 (1973)

Ribes, L.: Cohomological characterization of amalgamated products of groups. J. Pure Appl. Algebra **4**, 309–317 (1974)

Ribes, L.: Grupos Profinitos. Grupos Libres y Productos Libres. Monogr. Inst. Matem., vol. 5. UNAM, Mexico (1977)

Ribes, L.: Frattini covers of profinite groups. Arch. Math. **44**, 390–396 (1985)

Ribes, L.: The cartesian subgroup of a free product of profinite groups. Contemp. Math., Am. Math. Soc. **109**, 147–163 (1990)

Ribes, L.: Virtually free factors of pro-p groups. Isr. J. Math. **74**, 337–346 (1991)

Ribes, L., Steinberg, B.: A wreath product approach to classical subgroup theorems. Enseign. Math. (2010, to appear)

Ribes, L., Wong, K.: On the minimal number of generators of certain groups. Lond. Math. Soc. Lect. Notes **160**, 408–421 (1991)

Ribes, L., Zalesskii, P.A.: The pro-p topology of a free group and algorithmic problems in semigroups. Int. J. Algebra Comput. **4**, 359–374 (1994)

Ribes, L., Stevenson, K., Zalesskii, P.A.: On quasifree profinite groups. Proc. Am. Math. Soc. **135**, 2669–2676 (2007)

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

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

Roman'kov, V.A.: Width of verbal subgroups in solvable groups. Algebra Log. **21**, 60–72 (1982). English transl.: Algebra Log. **21**, 41–49 (1982)

Roman'kov, V.A.: Infinite generation of groups of automorphism of free pro-p groups. Sib. Mat. Zh. **34**, 153–159 (1993). English transl.: Sib. Math. J. **34**, 727–732

Romanovskii, N.S.: A generalized Freiheitsatz for pro-p groups. Sib. Math. Zh. **27**, 154–170 (1986)

Romanovskii, N.S.: On pro-p groups with a single defining relator. Isr. J. Math. **78**, 65–73 (1992)

Roquette, P.: On class field towers. In: Cassels, J.W.S., Fröhlich, A. (eds.): Algebraic Number Theory, pp. 231–249. Academic Press, London (1967)

Saxl, J., Wilson, J.S.: A note on powers in simple groups. Math. Proc. Camb. Philos. Soc. **122**, 91–94 (1997)

Ščepin, E.V.: The topology of limit spaces of uncountable inverse spectra. Russ. Math. Surv. **31**, 155–191 (1976)

Scott, P.: Subgroups of surface groups are almost geometric. J. Lond. Math. Soc. **17**, 555–565 (1978)

Scheiderer, C.: Real and Étale Cohomology. Lect. Notes Math., vol. 1588. Springer, Berlin (1994)

Scheiderer, C.: Farrel cohomology and Brown theorems for profinite groups. Manuscr. Math. **91**, 247–281 (1996)

Schirokauer, O.: A cohomological transfer map for profinite groups. J. Algebra **195**, 74–92 (1997)

Schmidt, A., Wingberg, K.: Šafarevič's theorem on solvable groups as Galois groups. Preprint (1998)

Segal, D.: Closed subgroups of profinite groups. Proc. Lond. Math. Soc. (3) **81**(1), 29–54 (2000)

Segal, D.: The finite images of finitely generated groups. Proc. Lond. Math. Soc. (3) **82**(3), 597–613 (2001)

Segal, D.: Words: notes on verbal width in groups. In: London Math. Soc. Lect. Notes Ser., vol. 361. Cambridge Univ. Press., Cambridge (2009)

Serre, J-P.: Structure de certains pro-p-groupes (d'après Demushkin). Sémin. Bourbaki 1962/1963, **252** (1963)

Serre, J-P.: Sur la dimension cohomologique des groupes profinis. Topology **3**, 413–420 (1965)

Serre, J-P.: Corps Locaux. Hermann, Paris (1968)

Serre, J-P.: Cohomologie des groupes discrets. Ann. Math. Stud., vol. 70, pp. 77–169. Princeton Univ. Press, Princeton (1971)

Serre, J-P.: A Course in Arithmetic. Springer, Berlin (1973)

Serre, J-P.: Trees. Springer, Berlin (1980)

Serre, J-P.: Topics in Galois Theory. Jones and Bartlett, Boston (1992)

Serre, J-P.: Cohomologie Galoisienne, 5th edn. Lect. Notes Math., vol. 5. Springer, Berlin (1995). The first edition was published in 1964

Shafarevich, I.R.: Construction of fields of algebraic numbers with given solvable groups. Izv. Akad. Nauk SSSR **18**, 525–578 (1954). English transl.: Am. Math. Soc. Transl. **4**, 185–237 (1956)

Shalev, A.: Characterizations of p-adic analytic groups in terms of wreath products. J. Algebra **145**, 204–208 (1992)

Shatz, S.S.: Profinite Groups, Arithmetic and Geometry. Princeton Univ. Press, Princeton (1972)

Shirvani, M.: On conjugacy separability of fundamental groups of graph of groups. Trans. Am. Math. Soc. **334**, 229–243 (1992)

SGA-1: Revêtements Étales et Groupe Fondamental. Lect. Notes Math., vol. 224. Springer, Berlin (1971)

Smith, J.H.: On products of profinite groups. Ill. J. Math. **13**, 680–688 (1969)

Steinberg, B.: Maximal subgroups of the minimal ideal of a free profinite monoid are free. Isr. J. Math. (2009, to appear)

Steinitz, E.: Algebraische Theorie der Körper. J. Reine Angew. Math. **137**, 167–309 (1910)

Suzuki, M.: Group Theory I. Springer, Berlin (1982)

Symonds, P.: Double coset formulas for profinite groups. Commun. Algebra **36**, 1059–1066 (2008)

Symonds, P., Weigel, T.: Cohomology of p-adic analytic groups. In: du Sautoy, M., Segal, D., Shalev, A. (eds.) New Horizons in Pro-p Groups, pp. 349–410. Birkhäuser, Boston (2000)

Tate, J.: Duality theorems in Galois cohomology over number fields. In: Proc. Int. Congress Math. Stockholm, pp. 288–295 (1962)

Uchida, K.: Isomorphisms of Galois groups. J. Math. Soc. Jpn. **28**, 617–620 (1976)

van den Dries, L., Ribenboim, P.: An application of Tarski's principle to absolute Galois groups of function fields. In: Proc. First Int. Symp. Ordered Algebraic Structures Luminy-Marseille 1984, pp. 131–148. Heldermann Verlag, Berlin (1986)

Völklein, H.: Groups as Galois Groups. An Introduction. Cambridge Univ. Press, Cambridge (1996)

Waterhouse, W.C.: Profinite groups are Galois groups. Proc. Am. Math. Soc. **42**, 639–640 (1972)

Weigel, T.: Maximal l-Frattini quotients of l-Poincaré duality groups of dimension 2. Arch. Math. (Basel) **85**(2005), 55–69 (2005)

Weigel, T., Zalesskii, P.A.: Profinite groups of finite cohomological dimension. C. R. Math. Acad. Sci. Paris **338**(5), 353–358 (2004)

Wilson, J.S.: Embedding theorems for residually finite groups. Math. Z. **174**, 149–157 (1980)

Wilson, J.S.: On the structure of compact torsion groups. Monatsh. Math. **96**, 57–66 (1983)

Wilson, J.S.: Profinite Groups. Clarendon Press, Oxford (1998)

Wilson, J.S.: On just infinite abstract and profinite groups. In: du Sautoy, M., Segal, D., Shalev, A. (eds.) New horizons in pro-p groups. Birkhäuser, Boston (2000)

Wilson, J.S., Zalesskii, P.A.: An embedding theorem for certain residually finite groups. Arch. Math. **67**, 177–182 (1996)

Würfel, T.: Extensions of pro-p groups of cohomological dimension two. Math. Proc. Camb. Philos. Soc. **99**, 209–211 (1986)

Zel'manov, E.I.: The solution of the restricted Burnside problem for groups of odd exponent. Izv. Akad. Nauk SSSR, Ser. Mat. **54**, 42–59 (1990). English transl.: Math. USSR Izv. **36**, 41–60

Zel'manov, E.I.: The solution of the restricted Burnside problem for 2-groups. Mat. Sb. **182**, 568–592 (1991)

Zel'manov, E.I.: On periodic compact groups. Isr. J. Math. **77**, 83–95 (1992)

Zel'manov, E.I.: On groups satisfying the Golod-Shafarevich condition. In: du Sautoy, M.P.F., Segal, D., Shalev, A. (eds.) New horizons in pro-p groups, pp. 223–232. Birkhäuser, Boston (2000)

Zubkov, A.N.: Nonabelian free pro-p-groups cannot be represented by 2-by-2 matrices. Sib. Mat. Zh. **28**, 64–69 (1987). English transl.: Sib. Math. J. **28**, 742–746

Index of Symbols

$(E_t^{r,s})_{r,s\in\mathbf{Z}}$ - spectral sequence, 397
cd - cohomological dimension, 251
$cd_p(G)$ - cohomological p-dimension, 251
$r_*(H)$ - rank function of H, 314
$r_p(G)$ - p-rank of G, 299
$r_S(G)$ - S-rank of G, 299
$rr(G)$ - relation rank, 281, 409
scd - strict cohomological dimension, 251
$scd_p(G)$ - strict cohomological p-dimension, 251
$tor(G)$ - torsion of G, 148, 264
tr - transgression map, 401
$\mathfrak{m}$-cardinal number, 90
$\mathrm{Tor}_n^{\Lambda}(A,-)$ - n-th derived functor of $A\widehat{\otimes}_{\Lambda}-$, 203
$\mathrm{Tot}(\mathbf{K})$ - total complex of a double complex, 405
$((IG))$ - augmentation ideal, 208
$(-)^G$ - fixed points functor, 204
$(-)_{\hat{\mathcal{C}}}$ - pro-$\mathcal{C}$ completion, 82
$(I,\preceq)$ - poset, 1
1_p - p-component of 1, 119
$1_{p'}$ - p'-component of 1, 119
$A[p]$ - kernel of multiplication by p, 252
$A\widehat{\otimes}_{\Lambda}B$ - complete tensor product, 177
$A_G(K)$ - subgroup of $\mathrm{Aut}(G)$ leaving K invariant, 132
$A_n(G)$ - group of automorphisms leaving invariant the n-th term of lower central series of G, 138
A_p - p-primary component of A, 226
$A_{\mathcal{C}}(G)$, $A(G)$ - relation module for a minimal presentation, 414
$arr(G)$ - relation rank as an abstract group, 289
B_G - $B/B((IG))$, 209
$C(X,Y)$ - space of continuous functions from X to Y, 58
$C^n(G,A)$ - homogeneous n-cochains, 207
C_n - cyclic group of order n, 16
$d(G)$ - minimal number of generators of G, 43
$def_{\mathcal{C}}(G)$, $def(G)$ - deficiency of a group, 415
$\dim H^n(G)$ - dimension over $\mathbf{F}_p$, where G is a pro-p group, 278
$d_F(K)$, 409
$d_F(K)$ - minimal cardinal of a generating set of K as normal subgroup, 279
$d_G(\tilde{K})$, 412
$E_2^{r,s}\Longrightarrow H^n$ - convergence of a spectral sequence, 399
e_B - edge morphism in a spectral sequence, 400
e_F - edge morphism in a spectral sequence, 401
$F(\mathfrak{m})$ - free pro-$\mathcal{C}$ group of rank $\mathfrak{m}$, 90, 314
$F_{\mathcal{C}}^r(X)$ - restricted free pro-$\mathcal{C}$ group, 89
$F_{\mathcal{C}}(X,*)$ - free pro-$\mathcal{C}$ group on a pointed profinite space $(X,*)$, 86
$F_{\mathcal{C}}(X)$ - free pro-$\mathcal{C}$ group on a profinite space X or on a set converging to 1, depending on context, 86, 89
Gx - G-orbit of x, 182
$G[n]$ - subset of elements of G of order dividing n, 65
$G\backslash X$ - quotient space of X modulo G, 182

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4,

G^* - dual group of G, 59
G^n - subset of n-powers of elements of G, 65
G^{**} - double dual of G, 59
$G_1 * G_2$ - abstract free product of groups, 354
$G_1 *_H G_2$ - abstract amalgamated free product, 368
$G_1 \amalg_H G_2$ - amalgamated free pro-$\mathcal{C}$ product, 368
G_a - stabilizer of a, 169
$G_{K/F}$ - Galois group of the field extension K/F, 68
$G_{\bar{F}/F}$ - absolute Galois group, 99
$G_{\hat{p}}$ - pro-p completion of G, 26
$G_{\hat{\mathcal{C}}}$ - pro-$\mathcal{C}$ completion of a group G, 26
$H \leq_c G$ - closed subgroup of G, 25
$H \leq_f G$ - subgroup of G of finite index, 25
$H \leq_o G$ - open subgroup of G, 25
$H \triangleleft_c G$ - closed normal subgroup of G, 25
$H \triangleleft_f G$ - normal subgroup of G of finite index, 25
$H \triangleleft_o G$ - open normal subgroup of G, 25
H^g - conjugate of H by g, 22
$H^n(G) = H^n(G, \mathbf{Z}/p\mathbf{Z})$, for G pro-p, 275
$H^n(G, A)$ - cohomology group, 203, 212
H_G - core of H in G, 22
$H_n(G, B)$ - homology group, 208
$J \subseteq_f I$ - finite subset of I, 29
$M(G)$ - intersection of all maximal normal subgroups of G, 304
$M_S(G)$ - intersection of all normal subgroups with quotient S, 299
$m \mid n$ - m divides n (as supernatural numbers), 33
$N_G(P)$ - normalizer of P in G, 39
$R^\times$ - multiplicative group of the ring R, 136
$R_p(G)$ - kernel of the maximal pro-p quotient of G, 96
$R_{\mathcal{C}}(G)$ - kernel of the maximal pro-$\mathcal{C}$ quotient of G, 96
$w_0(G)$ - local weight of G, 47
$w(G)$ - verbal subgroup, 121
$w(X)$ - weight of a topological space X, 47
$X - Y$ - set difference, 3
X/G - quotient space of X modulo G, 182
$Z(G)$ - center of G, 139
$[G : H]$ - index of H in G, 33
$[H, K]$ - subgroup generated by commutators, 55
$[h, k]$ - commutator, 55
$[RG]$ - abstract group algebra, 170
$[\Lambda X]$ - abstract free module on X, 167
$\#G$ - order of a profinite group G, 33
$\coprod_{i=1}^n G_i$ - free pro-$\mathcal{C}$ product of profinite groups, 353
$\cup$ - cup product, 282
δ, δ^n - connecting morphisms, 221
δ, δ_n - connecting morphisms, 196
$\gamma_n(G)$ - n-th term of lower central series, 41
Λ^{op} - opposite ring, 159
$\langle X \mid R \rangle$ - presentation, 409
$[\![RG]\!]$ - complete group algebra, 171
$[\![\Lambda(X, *)]\!]$ - free profinite Λ-module on a pointed profinite space $(X, *)$, 167
$[\![\Lambda X]\!]$ - free profinite Λ-module on a profinite space X, 167
$\varprojlim_{i \in I} X_i$ - inverse limit, 3
$\varinjlim A_i$ - direct limit, 15
$\overline{X}$ - closure of X, 41
$\overline{\langle X \rangle}$ - closed subgroup (submodule) generated by X, 42, 160
$\Phi(G)$ - Frattini subgroup, 53
$\Phi^n(G)$ - n-th term of the Frattini series of G, 57
π' - the set of primes not belonging to π, 35
$\prod$ - direct product, 2
$\rtimes$ - semidirect product, 41
$\varphi_{\hat{\mathcal{C}}}$ - homomorphism of pro-$\mathcal{C}$ completions induced by φ, 82
$|X|$ - cardinality of X, 48
$\widehat{G}$ - profinite completion of G, 26
$\{A_i, \varphi_{ij}, I\}$ - direct system, 14
$\{A_i, \varphi_{ij}\}$ - direct system, 14
$\{X_i, \varphi_{ij}, I\}$ - inverse system, 1

$\{X_i, \varphi_{ij}\}$ - inverse system, 1
$\mathbf{DMod}(G)$ - category of discrete G-modules, 170
$\mathbf{DMod}(\Lambda)$ - category of discrete Λ-modules, 165
$\mathbf{H}_\bullet$ - homological functor, 196
$\mathbf{H}^\bullet$ - cohomological functor, 195
$\mathbf{N}$ - set of natural numbers, 6
$\mathbf{PMod}(G)$ - category of profinite G-modules, 170
$\mathbf{PMod}(\Lambda)$ - category of profinite Λ-modules, 165
$\mathbf{Q}$ - field of rational numbers, 60
$\mathbf{R}$ - field of real numbers, 58
$\mathbf{T}$ - circle group, 58
$\mathbf{Z}$ - ring of integers, 6
$\mathbf{Z}_{\hat{\mathcal{C}}}$ - pro-$\mathcal{C}$ completion of $\mathbf{Z}$, 39
$\mathbf{Z}_p$ - ring of p-adic integers, 26
$\mathcal{C}(\Delta)$ - Δ-class, 21
$\mathcal{D}^{op}$ - opposite category to $\mathcal{D}$, 196
$\mathcal{E}$ - class of continuous epimorphisms, 98
$\mathcal{E}_f$ - class of homomorphisms with finite minimal kernel, 98
$\mathcal{K}_{\mathcal{N}}(G)$ - completion of G with respect to $\mathcal{N}$, 78
$\mathcal{N}^\ell$ - class of groups of Fitting length $\leq \ell$, 123
$\mathcal{S}_n$ - space of subgroups of order n, 264
$\mathcal{X}_{\mathcal{C}}(\mathfrak{m})$ - collection of all S-rank functions, 332
$\mathfrak{A}$ - category of abelian groups, 213
$\mathfrak{c}(G)$ - set of commutators of G, 121
$\mathfrak{m}^* = \max\{\mathfrak{m}, \aleph_0\}$, 294
$\mathfrak{w}(G)$, 120
$\mathrm{Ann}_{G^*}(H)$ - annihilator of H in G^*, 64
$\mathrm{Aut}(G)$ - automorphism group of G, 132
$\mathrm{Coind}_H^G(A)$ - coinduced module, 242
$\mathrm{Coinf} = \mathrm{Coinf}_{G/K}^G$ - coinflation map, 219
$\mathrm{Cor} = \mathrm{Cor}_G^H$ - corestriction map, 225, 229
$\mathrm{C}_G(k)$ - centralizer of k in G, 143
$\mathrm{Der}_L(H, A)$ - group of derivations vanishing on L, 375
$\mathrm{Der}(G, A)$ - group of derivations, 231
$\mathrm{End}(M)$ - group of continuous endomorphisms, 159
$\mathrm{Ext}_\Lambda^n(A, -)$ - n-th right derived functor of $\mathrm{Hom}_\Lambda(A, -)$, 201
$\mathrm{End}_\Lambda(M)$ - group of continuous Λ-endomorphisms, 159
gcd - greatest common divisor, 33
$\mathrm{HNN}^{abs}(H, A, f)$ - abstract HNN-extension, 382
$\mathrm{Hom}(M, N)$ - group of continuous homomorphisms, 159
$\mathrm{Hom}_\Lambda(M, N)$ - group of continuous Λ-homomorphisms, 159
$\mathrm{Ider}(G, A)$ - group of inner derivations, 231
$\mathrm{Im}(\varphi)$ - image of φ, 20
$\mathrm{Ind}_H^G(B)$ - induced module, 245
$\mathrm{Inf} = \mathrm{Inf}_G^{G/K}$ - inflation map, 215
id - identity map, 1
$\mathrm{Ker}(\psi)$ - kernel of ψ, 20
lcm - least common multiple, 33
$\mathrm{Pr}_n X$ - subset of elements represented as a product of length n of elements of X, 43
$\mathrm{Pr}_t(Y)$, 121
$\mathrm{Res} = \mathrm{Res}_H^G$ - restriction map, 224, 229
$\mathrm{rank}(F)$ - rank of a free pro-$\mathcal{C}$ group F, 90
$\mathrm{res}_K^G(M)$ - restriction of scalars, 248

Index of Authors

Abért, 389
Abrashkin, 291
Alperin, 40
Anderson, 154, 157, 351
Andreadakis, 157
Applegate, 73

Barnea, 117
Bary-Soroker, 351, 438
Bass, 118, 153
Baumslag, 373, 390
Bieri, 250
Binz, 117, 388
Bolker, 73
Borovik, 73
Bourbaki, 4, 18, 28, 58, 68, 70, 71, 75, 89, 127, 132, 181
Brauer, 73, 116
Bridson, 118
Brown, 250
Brumer, 193, 249

Camina, 391
Cartan, 195, 200, 201, 263, 264, 406
Chatzidakis, 117, 158, 194, 391
Cherlin, 73
Cossey, 73, 289, 438
Crawley, 157

Demushkin, 290
Deschamps, 194
Detomi, 74
Dicks, 390
Dikranjan, 59
Dixon, 73, 74, 116
Doerk, 127
Douady, 73, 91, 116, 249
du Sautoy, 73, 74
Dummit, 290

Efrat, 388
Eilenberg, 18, 195, 200, 201, 263, 264, 406
Ershov, 73, 388, 438
Evans, 157

Fernández-Alcober, 74
Fesenko, 291
Formanek, 116, 390
Fried, 73, 116
Fuchs, 18, 63, 129
Fujiwara, 391

Gaschütz, 73, 249, 289
Gildenhuys, 116, 157, 290, 351, 390
Gilotti, 73
Goldman, 193
Goldstein, 73
Golod, 289
González-Sánchez, 74
Grigorchuk, 391
Grothendieck, 117, 195, 200
Gruenberg, 73, 250, 289, 351, 438
Grunewald, 74, 116, 118, 291, 416
Gupta, 391
Guralnick, 73, 394, 416

Hall, M., 37, 38, 54–56, 116, 123, 124, 127, 140, 278, 303, 365
Hall, P., 37, 38, 157
Haran, 73, 289, 351, 388, 389, 394, 438
Harbater, 91, 116, 408, 436, 438
Hartley, 154
Hawkes, 127
Hegedűs, 389
Hensel, 73
Herfort, 73, 156–158, 289, 388–391
Hewitt, 51, 59, 129, 156
Higman, 118

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40, DOI 10.1007/978-3-642-01642-4,

Hillman, 416
Hochschild, 289
Hofmann, 59
Howson, 366
Huppert, 40, 41, 142, 148, 273, 289, 299

Ikeda, 157
Ivanov, 290
Iwasawa, 73, 116, 117

Jaikin-Zapirain, 74, 155, 291, 416
Jarden, 73, 116, 117, 351
Johnson, 391
Joly, 73

Kantor, 416
Kargapolov, 38, 149
Karras, 76, 368, 388
Kassabov, 118, 416
Kegel, 73, 289, 351, 438
Kharlampovich, 290
Kilsch, 116
Klaas, 73
Koch, 73
Kochloukova, 157, 291, 392
Koenigsmann, 388
Kovács, 73, 289, 389, 394, 438
Kropholler, 152, 157
Krull, 72

Labute, 290, 373
Lang, 73, 249, 250, 288
Larsen, 117
Lazard, 74, 153, 193
Leedham Green, 73
Leloup, 194
Leptin, 73
Lim, 73, 116, 194, 351
Linnell, 74, 157
Lubotzky, 73, 74, 117, 157, 158, 289, 351, 388–390, 392, 416
Lucchini, 74, 157, 389, 394
Lyndon, 95, 113, 290, 368, 388

Mac Lane, 66, 162, 165, 176, 179, 195, 200, 208, 221, 380, 406
Macintyre, 73
Magnus, 76, 368, 388
Mann, 73, 74
Martínez, 154
Matzat, 117
McCleary, 406
McMullen, 157, 158
Mel'nikov, 116, 117, 350, 351, 388, 389
Mennike, 153
Menegazzo, 157
Merzljakov, 38, 149
Morigi, 157
Morris, 59
Myasnikov, 290

Neukirch, 117, 157, 289, 388–390
Nikolov, 118, 120, 155, 393
Noskov, 74

Oltikar, 57, 73, 154, 351
Onishi, 73

Pappas, 194
Peterson, 154
Pickel, 116
Pinto, 157, 291, 416
Platonov, 118, 156, 392
Plesken, 73
Pletch, 154, 289, 291
Poitou, 73
Poland, 116
Pop, 117, 388
Prodanov, 59
Pyber, 73, 118

Rapinchuk, 153, 391
Remeslennikov, 290
Rhemtulla, 154
Rhodes, 438
Ribenboim, 73, 91
Ribes, 57, 73, 116, 154, 157, 243, 288, 289, 351, 388–390, 406, 438
Robinson, 149, 150, 152, 373
Roman'kov, 137, 155, 393
Romanovskii, 290
Roquette, 73, 289
Ross, 51, 59, 129, 156

Sah, 193
Saxl, 154
Ščepin, 194
Scheiderer, 194, 265, 289
Schirokauer, 249
Schmidt, 117, 289, 416
Schupp, 95, 113, 368, 388
Schur, 40

Scott, 116
Segal, 73, 74, 116, 118, 120, 155, 393
Serena, 73
Serre, 72, 113, 116, 117, 153, 154, 157, 193, 194, 243, 249, 250, 264, 265, 288–291, 327, 340, 358, 368–370, 388, 390, 393
Shafarevich, 116, 289
Shalev, 73, 74, 155
Shatz, 73, 193, 243
Shirvani, 390
Sidki, 391
Sim, 389, 394
Smith, 157
Solitar, 76, 368, 388
Steenrod, 18
Steinberg, 438
Steinitz, 73
Stevenson, 408, 436, 438
Stoyanov, 59
Strebel, 351
Suzuki, 304
Symonds, 250

Tate, 73, 249, 288
Tavgen, 118

Uchida, 157

van den Dries, 73, 91, 351
Verdier, 291
Vinberg, 289
Völklein, 117

Warhurst, 74
Waterhouse, 73
Weigel, 250, 289, 291
Wenzel, 117, 388
Wilson, 73, 152, 154–158, 289, 390, 391
Wingberg, 117
Wong, 389
Würfel, 290

Zalesskii, 116, 289, 291, 391, 416, 438
Zassenhaus, 40
Zel'manov, 154–157, 289
Zubkov, 117

Index of Terms

G-number, 73
G-decomposition, 182
G-homomorphism, 170
G-map, 182
G-module, 169
G-orbit, 182
G-quotient space, 182
G-space, 180
– free, 182
– with no continuous section, 188
G-stabilizer, 182
p-complement, 38
p-element, 120
p-primary abelian group, 251
p-rank, 299
S-rank, 299
π-number, 35
$\mathcal{E}$-embedding problem, 99

absolute Galois group of a field, 99
accessible
– chain, 302
– subgroup, 302
action
– diagonal, 190
– fixed-point-free, 142
– free, 182
admissible class of epimorphisms, 99
algebra
– profinite, 177
amalgamated free product, 367
– example of nonproper, 372
– proper, 369
analytic pro-p group, 73
annihilator, 64
augmentation
– ideal, 208
– map, 205, 206
automorphism
– lifting automorphisms of quotients, 350
– normal, 157

base terms (of a spectral sequence), 400
basis
– converging to 1, 90
– of a module, 168
– topological, 88
bifunctor, 200
bigraded abelian group, 397
– differential of a, 397
bimodule, 180
Boolean space, 9
boundary, 208
bounded generation, 391

cartesian product, 2
cartesian subgroup, 357
circle group, 58
class of finite groups, 19
– $\mathcal{C}(\varDelta)$, 21
– $\varDelta$-class, 21
– closed under extensions, 20
clopen set, 9
coboundary, 207, 213
cochain, 207
cocycle, 207, 213
coeffaceable, 197
cofinal, 8
– subsystem, 8
cohomological p-dimension, 251
cohomology group
– functorial behavior, 214
– of a complex, 199
– of a group, 203, 212
cohomology group of a group
– as a derived functor, 220

L. Ribes, P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40,
DOI 10.1007/978-3-642-01642-4,

coinduced module, 243
coinflation, 219
commutator subgroup, 341
compact-open topology, 58, 134, 162, 181
compatible
– maps, 2, 14, 214
– pairs of maps, 162
completion, 78
– as functor, 81
– pro-$\mathcal{C}$ completion, 26
complex
– filtered, 403
component of a map of direct systems, 17
congruence
– kernel of $\mathrm{SL}_2(\mathbf{Z})$, 340
– subgroup, 153
– subgroup problem, 153
– subgroup topology, 153, 340
congruence subgroup topology of $\mathrm{Aut}(G)$, 132
connecting homomorphism, 221
connecting morphism, 195
convergence to 1
– of a map, 88, 160
– of a subset, 160
convergence to 1
– of a subset, 42
convergent
– family of maps, 425
coproduct of spaces, 294
core of a subgroup, 22
corestriction
– in cohomology, 225
– in homology, 229
covariant cohomological functor, 195
crossed homomorphism, 231
– principal, 231
cup product, 282
cycle, 208

deficiency, 415
– of a presentation, 414
Demushkin group, 290
derivation, 231
– inner derivation, 231
differential
– bidegree of a, 397
direct
– constant system, 14
– limit, 14
– system, 14
direct product, 2
direct sum of modules, 162
discrete G-module, 169
divisible abelian group
– structure, 129
double complex, 405
– first spectral sequence of, 405
– second spectral sequence of, 405
– total complex of a, 405
duality
– of modules, 165
– Pontryagin, 59

edge homomorphisms on the fiber, 401
effaceable, 197
embedding problem
– proper, 407
– solvable, 99
– split, 407
– weakly solvable, 99
enough injectives, 175
enough projectives, 174
equivalence relation
– closed, 10
– intersection of, 11
– open, 10
exact sequence, 20
– equivalence, 233
extension
– of profinite groups, 233
– split, 93, 235

factor system, 233
fiber terms (of a spectral sequence), 400
filtered abelian group, 398
– grading of a, 399
filtered from below, 24
filtered graded abelian group, 399
filtration, 398
– bounded, 404
– first filtration of a total complex, 405
– of a complex, 403
– second filtration of a total complex, 405
first axiom of countability, 11

fixed subgroup
– M^U, 169
fixed submodule, 204
formation, 20
– NE-formation, 20
Frattini
– quotient, 53
– series, 57
– subgroup, 53
free
– factor, 355
– pro - $\mathcal{C}$ product, 353
– product with amalgamation, 367
– – example of nonproper, 372
– – proper, 369
– profinite group, 86
free pro - $\mathcal{C}$ product, 425
– and absolute Galois groups, 388
freely indexed group, 311
Frobenius
– automorphism, 71
– complement, 142
– group, 142
– kernel, 143
functor
– coeffaceable, 197
– cohomological, 195, 196
– derived, 199
– effaceable, 197
– exact, 31
– Ext, 201
– homological, 196
– left exact, 199
– positive effaceable cohomological, 197
– right exact, 199
– Tor, 203
– universal (co)homological, 197

generators
– as a normal subgroup, 279
– converging to 1, 42
– of a group vs its profinite completion, 74
– of a profinite group, 42
– topological, 42
group
– Δ-group, 20
– π-group, 35
– divisible, 65
– dual group, 59
– finite generation of profinite, 42
– free on a profinite space, 86
– free pro - $\mathcal{C}$ on a set converging to 1, 89
– freely indexed, 311
– Hopfian, 44
– LERF, 116
– of finite exponent, 129
– operating on a group, 181
– operating on a space, 180
– pro - $\mathcal{C}$, 19
– pro - π group, 35
– pro-p, 20
– proabelian, 20
– procyclic, 20, 51
– profinite, 20
– profinite dihedral group, 143
– profinite homogeneous, 314
– pronilpotent, 20
– prosolvable, 20
– quasicyclic, 16
– residually $\mathcal{C}$, 75
– residually finite, 76
– restricted free profinite, 89
– S-group, 21
– structure of divisible abelian, 129
– subgroup separable, 116
– supersolvable, 56
– torsion, 129
group algebra, 170
– complete, 171
group ring, 170

Hall subgroup, 35
HNN-extensions of pro - $\mathcal{C}$ groups, 382
– proper, 383
homogeneous group, 314
homology group
– functorial behavior, 214
– of a group, 208
homology groups of a group as derived functors, 208
Hopfian group, 44

index of a subgroup, 33
induced module, 245
inductive
– limit, 14

– system, 14
inflation map, 215
injective
– enough injectives, 175
– object, 175
inverse
– constant system, 1
– limit, 2
– limit of projective groups, 275
– projection map of inverse limit, 2
– short exact sequence of inverse systems, 31
– system, 1
inverse problem of Galois theory, 100

just-infinite, 155

Krull topology, 68
Kurosh system, 428
– existence, 428

length of a module, 253
lifting, 172
limit
– direct, 14
– inductive, 14
– inverse, 2
– projective, 2
limit pro-p group, 392
Lyndon-Hochschild-Serre spectral sequence, 258

Magnus algebra, 193
map
– converging to 1, 88, 160
– middle linear, 177
– of direct systems, 17
– of inverse systems, 4
maps
– compatible pair of, 162
Mayer-Vietoris sequence, 374
minimax group, 149
module, 159
– basis of free, 168
– cofree, 175
– coinduced, 243
– discrete, 165
– finitely generated, 160
– free profinite, 166
– G-module, 169
– induced, 245
– Λ-module, 159
– profinite, 165
– simple, 252
– with trivial action, 169
modules
– direct sum of, 162
morphism
– of cohomological functors, 196
– of G-modules, 170
– of Λ-modules, 159

net, 119
– cluster point of a, 119
– convergence of a, 119
Nielsen-Schreier theorem, 114
nongenerator, 53

order of a profinite group, 33

partially ordered set, 1
– directed, 1
Poincaré Group, 290
polycyclic group, 152
pontryagin duality, 59
poset, 1
– cofinal subset, 8
presentation, 409
– finite, 409
– minimal, 409
– of a pro-p group, 281
pro-$\mathcal{C}$ topology of a group, 75
– full, 75
pro-$\mathcal{C}$ group, 19
pro-p group, 20
– with one relator, 290
proabelian group, 20
procyclic group, 20, 51
profinite
– dihedral group, 143
– free group, 86
– free group on a set converging to 1, 89
– G-module, 169
– group, 20
– metrizable profinite group, 51
– module, 165
– order of a profinite group, 33
– restricted free group, 89
– ring, 159

– space, 9
– strongly complete group, 120
– topology, 75, 76
– torsion group, 156
profinite groups with the same finite quotients, 85
projection
– of an inverse limit, 2
projective
– $\mathcal{C}$-projective profinite group, 271
– enough projectives, 174
– limit, 2
– object, 172
– profinite group, 271
– solvable profinite group, 278
– system, 1
pronilpotent group, 20
prosolvable group, 20
Prüfer group, 16
pullback, 66
pure subgroup, 129
pushout, 67

quasisimple finite group, 416

rank
– of a free group, 90
– S-rank function of a group, 314
– S-rank of a profinite group, 299
relation module, 412
relation rank, 281, 409
relator
– defining relators, 281
residually $\mathcal{C}$ group, 75
residually finite group, 76
resolution
– homogeneous, 206
– inhomogeneous, 206
– injective, 199
– projective, 200
– split, 211
restriction
– in cohomology, 224
– in homology, 229
restriction of scalars, 248
ring
– commutative profinite, 161
– profinite, 159

Schreier's formula, 311
Schur-Zassenhaus theorem, 40
second axiom of countability, 11
section
– for G-spaces, 184
– of a map, 29
semidirect product, 41
– external, 181
sequence
– exact, 20
– of inverse systems, 31
– short exact sequence of groups, 20
series
– derived, 341
– lower central, 41
– lower p-central series, 57
Shapiro's Lemma, 244, 245
space
– Boolean, 9
– countably based, 11
– first countable, 11
– pointed, 85
– profinite, 9
– second countable, 11
– totally disconnected, 4
– weight of a, 47
spectral sequence, 397
– base terms, 400
– convergence, 399
– edge homomorphisms, 400, 401
– fiber terms, 400
– first quadrant, 399
– initial term, 398
– Lyndon-Hochschild-Serre, 258
– of a double complex, 405
– of a filtered complex, 402
– positive, 399
splitting, 238
– T-splitting of sequence, 238
stabilizer, 169
strict cohomological p-dimension, 251
strong lifting property, 99
strongly complete profinite group, 120, 122
– example of a nonstrongly complete group, 127
subdirect product, 19
subgroup
– accessible, 302

– cartesian, 357
– characteristic, 44
– derived, 341
– isolated, 142
– of a free pro - $\mathcal{C}$: not free, 331
– pure, 129
– subnormal, 115
– subnormal in free pro-$\mathcal{C}$ groups, 336
– verbal, 96
subgroups of finite index
– in profinite groups, 122
submodule
– of fixed points, 204
supernatural number, 33, 73
– divides, 33
– greatest common divisor of, 33
– least common multiple of, 33
– product of, 33
Sylow
– subgroup, 35
– theorem, 37
tensor product
– commutes with $\varprojlim$, 178
– complete, 177
torsion subset, 148
transfer, 225
transgression, 401
transversal, 22
– Schreier transversal, 114
trivial action, 169

variety of finite groups, 20
– extension closed, 20
– saturated, 272
verbal subgroup, 120

weight
– local, 47
– of a space, 47
width of a word w, 121

Zassenhaus group, 278