PROFINITE GROUPS, ARITHMETIC, AND GEOMETRY

BY

STEPHEN S. SHATZ

ANNALS OF MATHEMATICS STUDIES
PRINCETON UNIVERSITY PRESS

Annals of Mathematics Studies

Number 67

PROFINITE GROUPS, ARITHMETIC, AND GEOMETRY

BY

STEPHEN S. SHATZ

PRINCETON UNIVERSITY PRESS

AND

UNIVERSITY OF TOKYO PRESS

1972

Copyright © 1972, by Princeton University Press
ALL RIGHTS RESERVED
LC Card: 77-126832
ISBN: 0-691-08017-8
AMS 1968: Primary—2050, 2051, 1067, 1068
Secondary—1015, 1077, 1078,
1435, 1440, 1810, 1815, 1820, 5532

Published in Japan exclusively by
University of Tokyo Press;
in other parts of the world by
Princeton University Press

Printed in the United States of America

For Marilyn, Geoffrey, and Adria

PREFACE

This short volume reproduces in its first five chapters the essential content of a one semester course I gave at the University of Pennsylvania in the Spring of 1968. The last chapter covers material I had hoped to include, but could not for lack of time. My aim in giving such a course was to give students a body of material upon which some of the modern research in Diophantine geometry and higher arithmetic is based, and to do this in a way which emphasized the many interesting roads out of these elementary foundations. I wanted to enable them to start reading the literature in those areas of mathematics I personally find very interesting. The enthusiastic reception of my able class convinced me that this material was deserving of a larger audience, and I resolved to write up the notes for the course.

Anyone conversant with this subject will note how indebted I am to many authors. Foremost among them is J. P. Serre from whose works I have taken a great deal,* and there is John Tate whose unpublished work and unmistakeable stamp appear here in many places. Responsibility for any errors is, of course, my own.

The highly personal nature of these notes has not blinded me to their many faults, notably the lack of good examples and exercises, and the uneven tempo of exposition. In attempting to retain the flavor of the original lectures, I have allowed these and other faults to stand; I hope they do not vitiate the aim of the project. I have also included a large but not exhaustive bibliography; it covers the main references, and the bibliographies in these works and will serve as a good guide to the literature.

* Especially from [SCL, SG] where the smooth treatment is impossible to improve upon.

CONTENTS

PREFACE vii

CHAPTER I – PROFINITE GROUPS

§0. Preliminaries on Projective and Inductive Limits 3

§1. Profinite Groups 7

§2. Supernatural Numbers and the Sylow Theory 12

CHAPTER II – COHOMOLOGY OF PROFINITE GROUPS

§1. δ-functors and the Definition of the Cohomology of Profinite Groups 16

§2. Behavior of the Cohomology as a Functor, Induced Modules 23

§3. Restriction, Transfer (co-restriction), and Cup-products 33

§4. A Utilitarian View of Spectral Sequences 39

CHAPTER III – COHOMOLOGICAL DIMENSION

§1. Definition and Elementary Properties 53

§2. The Case of Cohomological Dimension One 63

§3. The Structure of Profinite p-groups; Šafarevič-Golod's Theorem 69

§4. Šafarevič's Solution of the Class Tower Problem 86

CHAPTER IV – GALOIS COHOMOLOGY AND FIELD THEORY

§1. Resume of Krull's Galois Theory and First Results 93

§2. The Cohomological Dimension of Fields 97

§3. Algebraic Dimension, Quasi-algebraic Closure, and the Property C_r 101

§4. Existence of Fields of Arbitrary Cohomological Dimension 119

§5. Counter-examples in the Theory of Cohomological Dimension and Forms 121

CHAPTER V – LOCAL CLASS FIELD THEORY

§1. Local Fields and Their Extensions – A Resumé 129

§2. Cohomological Triviality, Tate and Nakayama Theorems, and Herbrand Quotients 136

§3. The Brauer Group of a Local Field 152

§4. The Existence Theorem (Part I: Formal Existence Theorem, and beginning of the proof.) 166

§5. The Existence Theorem (Part II: The Hilbert Symbols and completion of the proof.) 173

CHAPTER VI – DUALITY

§1. Dualizing Modules and Poincaré Groups 183

§2. Grothendieck Topologies and Cohomology 192

§3. Galois, Étale, and Flat Cohomology 204

§4. Finite Group Schemes and Their Cohomology Over a Local Field 217

§5. Tate-Nakayama Duality 230

§6. Duality Theorem for Finite Group Schemes 236

BIBLIOGRAPHY 248

PROFINITE GROUPS, ARITHMETIC, AND GEOMETRY

CHAPTER I

PROFINITE GROUPS

§0. Preliminaries on projective and inductive limits*

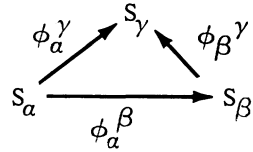
Let Λ be a set (the index set) and suppose S_α, for $\alpha \in \Lambda$ is a family of sets (groups, rings, etc.) indexed by Λ. We assume Λ is partially ordered (by $\alpha \leqq \beta$) and satisfies the

Moore-Smith Property: $(\forall \alpha, \beta)(\exists \gamma)(\alpha \leqq \gamma \text{ and } \beta \leqq \gamma)$.

Now we assume given the following data:

$$(1) \qquad (\forall \alpha, \beta)(\alpha \leqq \beta \Longrightarrow \exists\, \phi_\alpha^\beta : S_\alpha \to S_\beta) \ ,$$

and the maps (group-homomorphisms, ring homomorphisms, etc.) are *consistent* in the sense that: given α, β, γ with $\alpha \leqq \beta \leqq \gamma$, then the induced diagram



commutes. Furthermore, we insist that $\phi_\alpha^\alpha = \mathrm{id}$, all α.

Any system, as above, will be called a *direct mapping family* of sets (groups, rings), and denoted $\{S_\alpha, \phi_\alpha^\beta\}$. From now on, we will concentrate on the set-theoretic formulation, leaving to the reader the task of formulating all definitions and results for groups, rings, or objects of other categories.

* Only the concept of lim based on a directed index set, not on the more general notion of "index category," is introduced here.

If instead of the equation (1), we write

$$(2) \qquad (\forall \alpha, \beta)(\alpha \leqq \beta \implies \exists \phi_\beta^\alpha : S_\beta \to S_\alpha)$$

and demand the obvious consistency, we get a *projective (or inverse) mapping family* of sets (etc.) —this time with the notation

$$\{S_\alpha, \phi_\beta^\alpha\} .$$

Examples. (1D) $S_\alpha = \mathbf{Z}$, Λ = natural numbers: $1, 2, \ldots$, and the ordering on Λ is by cardinality (i.e., the usual ordering). $\phi_n^{n+1} : \mathbf{Z} \to \mathbf{Z}$ is "multiplication by p," where p is a fixed prime number.

(1P) Same as (1D), only in this case ϕ_{n+1}^n is multiplication by p.

(2D) Λ = natural numbers, partially ordered by division. $S_n = \mathbf{Z}/n\mathbf{Z}$, and if $n \leqq m$ (i.e., $n|m$), then ϕ_n^m is multiplication by m/n.

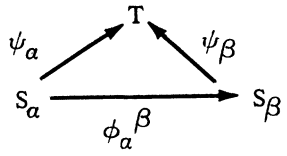
(2P) Same S_n and Λ as (2D). This time ϕ_m^n is the natural projection $\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$.

(3D) G is a group; Λ is the family of all finite subgroups of G, partially ordered by inclusion. S_α is α considered as subgroup of G, not as element of Λ. The map ϕ_α^β is the natural inclusion $S_\alpha \to S_\beta$.*

(3P) G is a group, Λ is the family of all normal subgroups of G of finite index. If α is in Λ, S_α is G/α, a finite group. Partially order Λ *via*: $\alpha \leqq \beta \iff \beta \subseteq \alpha$ as subgroups; let ϕ_β^α be the natural projection $S_\beta \to S_\alpha$. (Observe (3P) generalizes (2P).)

If T is a set, and if $\psi_\alpha : S_\alpha \to T$ are given maps, one for each $\alpha \in \Lambda$, which are consistent with the ϕ_α^β in the sense that the diagram

(3)



commutes for all $\alpha \leqq \beta$; then we may inquire as to how "faithfully $\{T, \psi_\alpha\}$ possesses all the information contained in $\{S_\alpha, \phi_\alpha^\beta\}$"? More exactly,

* We assume G is abelian.

we may ask: Does there exist a "universal" object $\{T, \psi_\alpha\}_{\alpha \in \Lambda}$ from which the others may be recaptured? (For projective systems the ψ_α take T to S_α for all α, and the diagram is changed *mutatis mutandis*.) As is usual in such circumstances, what we are asking for is the *representability of a certain functor* —or, in older terminology, the *solution of a universal mapping problem*. The functor we wish to represent is F where

$$F(T) = \{\text{families } \{\psi_\alpha\}_{\alpha \in \Lambda} \mid \psi_\alpha : S_\alpha \to T \text{ and}$$

$$\text{diagram (3) commutes for all } \alpha \leqq \beta\} .$$

The representing object will then be a set S and a "universal" family $\{\phi_\alpha\}_{\alpha \in \Lambda}$, where $\phi_\alpha : S_\alpha \to S$ and the ϕ_α are consistent. In terms of universal mapping properties, the object we seek will have the

Direct universal mapping property (DUMP):

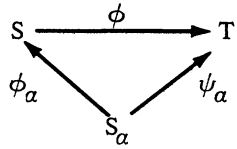
(a) $\{S, \phi_\alpha\}_{\alpha \in \Lambda}$ is a set and a consistent family indexed by Λ; $\phi_\alpha : S_\alpha \to S$ and

(b) Given any other pair $\{T, \psi_\alpha\}_{\alpha \in \Lambda}$ having (a), *there exists a unique* map

$$\phi : S \to T$$

so that the diagram

(4)



commutes for every $\alpha \in \Lambda$.

(The reader may formulate the analogous universal mapping problem for inverse families by turning arrows around and so arrive at a formulation of the *Projective universal mapping property* (PUMP).)

Again, as is usual, if the objects we seek exist then they will be unique up to unique isomorphism. Any object satisfying the DUMP is called the

direct limit of the family $\{S_\alpha, \phi_\alpha^\beta\}$ —by abuse of notation it is written

$$S = \operatorname{dir}\lim_\alpha S_\alpha .$$

Similarly, any object satisfying the PUMP is the *projective limit* of the family $\{S_\alpha, \phi_\beta^\alpha\}$ —written

$$S = \operatorname{proj}\lim_\alpha S_\alpha .$$

For our purposes, the following theorem is sufficient.

THEOREM 1. *In the categories of sets, groups, rings, and topological groups, direct and inverse limits always exist.*

Proof: We content ourselves with a sketch—and that only for the case of sets. The other categories are entirely similar and obvious modifications of our proof yield the desired results.

Let $\{S_\alpha, \phi_\alpha^\beta\}$ be a direct mapping family of sets. We may and do assume that the S_α are disjoint, and we form their union $\mathcal{S} = \bigcup_\alpha S_\alpha$. In $\mathcal{S}$ introduce the relation, $\sim$, by:

If $x \in \mathcal{S}$, $y \in \mathcal{S}$, (say $x \in S_\alpha$, $y \in S_\beta$) then $x \sim y$ if and only if $(\exists \gamma)(\alpha \leqq \gamma, \beta \leqq \gamma)$ such that $\phi_\alpha^\gamma(x) = \phi_\beta^\gamma(y)$.

One sees trivially that $\sim$ is an equivalence relation, and we may form $S = \mathcal{S}/\sim$. Let $\phi_\alpha : S_\alpha \to S$ be the composition: $S_\alpha \to \mathcal{S} \to \mathcal{S}/\sim$. It is easily checked that $\{S, \phi_\alpha\}_{\alpha \in \Lambda}$ has the DUMP.

Now let $\{S_\alpha, \phi_\beta^\alpha\}$ be an inverse mapping family of sets. Form the cartesian product $X = \prod_\alpha S_\alpha$. Let S be the subset of X consisting of all *consistent* tuples (x_α) i.e.,

$$(x_\alpha) \in S \iff (\forall \beta, \gamma)(\beta \leqq \gamma \implies \phi_\gamma^\beta(x_\gamma) = x_\beta) .$$

Let ϕ_α be the αth projection restricted to S. One checks that $\{S, \phi_\alpha\}_{\alpha \in \Lambda}$ has the PUMP. (Note: It may happen that $S = \emptyset$.) Q.E.D.

Examples. These examples refer to the earlier ones on page 4.

(1D) $\operatorname{dir\,lim}_n \{S_n, \phi_n^{n+1}\} = \{\frac{r}{p^s} \mid r, s \in \mathbf{Z}\}$

(1P) $\operatorname{proj\,lim} \{S_n, \phi_{n+1}^{n}\} = (0)$

(2D) $\operatorname{dir\,lim} \{S_n, \phi_n^{m}\} = \mathbf{Q}/\mathbf{Z}$

(2P) $\operatorname{proj\,lim} \{S_n, \phi_m^{n}\} = \hat{\mathbf{Z}}$ = "completion of $\mathbf{Z}$ in the ideal topology"

$\cong \Pi_p \mathbf{Z}_p$, where $\mathbf{Z}_p$ is the ring of p-adic integers.

(3 D) If G is abelian, $\operatorname{dir\,lim}_\alpha S_\alpha$ is the torsion subgroup of G.

(3 P) $\operatorname{proj\,lim}_\alpha S_\alpha$ is called the *"strong" completion* of G.

§1. Profinite Groups

DEFINITION 1. A *profinite group* is a projective limit of finite groups.

Observe that examples (2P) and (3P) are profinite groups. From the proof of Theorem 1, since every finite group is a compact, Hausdorff group, one sees that *the projective limit of finite groups is, in a natural way, a compact Hausdorff group.* The following theorem specifies how we may isolate the profinite groups from among all compact groups.

THEOREM 2. *The following conditions are equivalent.*

(1) G *is a profinite group.*

(2) G *is a compact, Hausdorff group in which the family of open normal subgroups forms a fundamental system of neighborhoods at* 1.

(3) G *is a compact, totally disconnected, Hausdorff group.*

Proof: (1) $\Longrightarrow$ (2). Since G is profinite, there are finite groups G_α and maps $\phi_\beta^\alpha : G_\beta \to G_\alpha$ such that $G = \operatorname{proj\,lim}_\alpha G_\alpha$. Hence, there are maps $\phi_\alpha : G \to G_\alpha$, for all α. Let $U_\alpha = \ker \phi_\alpha$, then the U_α are open, normal

subgroups of G. Clearly, (2) will hold if we succeed in proving that $\bigcap_\alpha U_\alpha = \{1\}$. But, if $\xi \in U_\alpha$ for every α, then using the explicit form of G gotten from the proof of Theorem 1, one sees that ξ as a tuple has α^{th} projection 1 everywhere. It follows immediately that $\xi = 1$, as required.

(2) $\Longrightarrow$ (3). Let N be the connected component of identity in G. If $\{U_\alpha\}$ denotes the family of all open, normal subgroups of G, let $N_\alpha = U_\alpha \cap N$ for all α. The groups N_α are open, normal subgroups of N; as N is connected, we must have $N_\alpha = N$ for all α. But then

$$N = \bigcap_\alpha N_\alpha = \bigcap_\alpha N \cap U_\alpha = N \cap \bigcap_\alpha U_\alpha = N \cap \{1\} .$$

(The last equality by hypothesis (2).) Thus $N = \{1\}$, and (3) is proved.

(3) $\Longrightarrow$ (1). It follows from our hypothesis, and fromTheorem 17, Chapter III of [P], that given any open neighborhood U of 1 in G, there exists an open subgroup H of G with $H \subseteq U$. Since G is compact and H is open, the index $(G:H)$ is finite, and therefore $(G: N_G(H)) < \infty$. From this, it follows that the distinct conjugates $x H x^{-1}$ of H in G are finite in number, so their intersection K forms an open, normal subgroup of G contained in H; hence, in U. As U was an arbitrary open neighborhood of 1, we see that the intersection of all open, normal subgroups of G reduces to the identity. Let $\{U_\alpha\}$ denote the family of all open, normal subgroups of G (so that we have shown $\bigcap_\alpha U_\alpha = \{1\}$). The groups $G/U_\alpha = G_\alpha$ form in a natural way a projective mapping family of *finite* groups. Our theorem now follows from the more general

LEMMA 1. *Let* G *be a compact, Hausdorff group; let* G_α, S_α *be two families of closed subgroups of* G, *indexed by the directed set* Λ. *Assume that* $S_\alpha \lhd G_\alpha$ *for all* α; *and that for* $\beta \geq \alpha$, $G_\alpha \supseteq G_\beta$ *and* $S_\alpha \supseteq S_\beta$. *Then the groups* $H_\alpha = G_\alpha/S_\alpha$ *form a projective mapping family in a natural way, and*

$$\operatorname*{proj\,lim}_\alpha H_\alpha = \operatorname*{proj\,lim}_\alpha G_\alpha/S_\alpha = \bigcap_\alpha G_\alpha / \bigcap_\alpha S_\alpha \quad .$$

Proof: If $\beta \geq \alpha$, then $S_\beta \subseteq S_\alpha$; so one has the maps

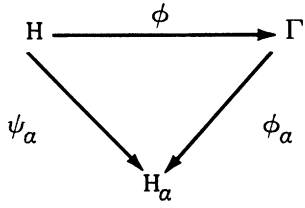
$$\phi_\beta^{\alpha}: H_\beta = G_\beta / S_\beta \to G_\alpha / S_\alpha = H_\alpha$$

given by $\phi_\beta^{\alpha}(xS_\beta) = xS_\alpha$. The consistency of these maps is trivial. Let $\Gamma = \operatorname{proj}\lim_{\alpha} H_\alpha$, and let $\phi_\alpha: \Gamma \to H_\alpha$ be the canonical homomorphisms. There are obvious maps $\psi_\alpha: \bigcap G_\beta / \bigcap S_\beta = H \to H_\alpha$, for each α and they are consistent with the ϕ_β^{α}. Hence, by the PUMP, we obtain a map

$$\phi: H = \bigcap G_\alpha / \bigcap S_\alpha \to \Gamma \ .$$

Here, map means continuous group homomorphism, so when ϕ is proven bijective the compact Hausdorff property of the groups in question will show that ϕ is automatically a homeomorphism.

Let $\xi \in H$, and assume $\phi(\xi) = 1 \in \Gamma$. The diagram



shows that $\psi_\alpha(\xi) = 1$ for all α. Thus $\xi \in S_\alpha$ for all α; hence, ξ represents 1 in H and ϕ is injective. Given $x \in \Gamma$, let $x_\alpha = \phi_\alpha(x) \in H_\alpha$ for each α. As H_α is G_α / S_α, there exists a $\xi_\alpha \in G_\alpha$ such that $\xi_\alpha \bmod S_\alpha$ is x_α. The net $\{\xi_\alpha\}_\alpha$ possesses a converging subnet $\{\xi_{\alpha_\nu}\}_\nu$ because all the ξ_α lie in G and G is compact. Let $\tilde{\xi}$ be the limit of this subnet. Now given any α, the set of all α_ν with $\alpha_\nu \geq \alpha$ is final in the α_ν; hence, $\lim_{\alpha_\nu \geq \alpha} \xi_{\alpha_\nu} = \tilde{\xi}$. But $\xi_{\alpha_\nu} \in G_{\alpha_\nu} \subseteq G_\alpha$ if $\alpha_\nu \geq \alpha$, and as G_α is closed in G, we deduce that $\tilde{\xi} \in G_\alpha$. Thus $\tilde{\xi} \in \bigcap_\alpha G_\alpha$. Let ξ be the coset of $\tilde{\xi}$ mod $\bigcap_\alpha S_\alpha$, i.e., $\xi \in H$. All we need now show is $\psi_\alpha(\xi) = x_\alpha$ for every α. This is very easy as follows: The x_α are consistent; hence, for all $\beta \geq \alpha$, $\xi_\beta \bmod S_\alpha = \xi_\alpha \bmod S_\alpha$. Given any α, for any $\beta \geq \alpha$, we can find

$s_{\alpha\beta} \in S_\alpha$ with $\xi_\beta = \xi_\alpha s_{\alpha\beta}$. The $\{s_{\alpha\beta}\}_\beta$ form a net in S_α, so there is a converging subnet. Look at the subnet of this newly chosen subnet formed by those β beyond some number α_ν of our previous indexing set. We have

$$\lim_{\substack{\beta \text{ in new} \\ \text{family}}} s_{\alpha\beta} = s_\alpha \in S_\alpha,$$

and hence,

$$\tilde{\xi} = \lim_\beta \xi_\beta = \lim_\beta \xi_\alpha s_{\alpha\beta} = \xi_\alpha s_\alpha .$$

The last equation when unscrambled in terms of $\tilde{\xi}$ and ψ_α says precisely $\psi_\alpha(\tilde{\xi}) = x_\alpha$. Q.E.D.

Here are some facts concerning profinite groups whose proofs are easy exercises.

(Fact 1) Every closed subgroup and every quotient group of a profinite group is profinite.

(Fact 2) The product or projective limit of a family of profinite groups is profinite.

(Fact 3) If S is any subgroup of a profinite group G, then its closure $\bar{S}$ is given by

$$\bar{S} = \bigcap \{U \mid U \text{ is an open normal subgroup of } G \text{ and } S \subseteq U\}.$$

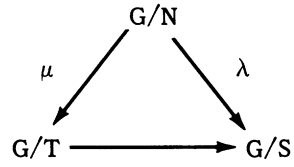
(Fact 4) If G is an abelian group, then G is profinite if and only if its Pontrjagin dual is a torsion group. In this way, the category of profinite abelian groups is the dual of the category of torsion abelian groups.

An important theorem for the cohomology theory of profinite groups is:

THEOREM 3. (Cross-section Theorem) *Let* G *be a profinite group and let* N *be a closed normal subgroup. Then there exists a continuous cross-section for the map* $\pi : G \to G/N$. *That is, there is a continuous map* $\phi : G/N \to G$ *(not a homomorphism in general) such that* $\phi(x) \in x$ *or, equivalently,* $\pi(\phi(x)) = x$.

Proof: Let $\mathfrak{S}$ be the set of all *closed* normal subgroups S of G such that $S \subseteq N$. Consider pairs $<S, \lambda>$ where $\lambda: G/N \to G/S$ is a cross-section (continuous of course) of the projection $G/S \to G/N$. Call the set of such pairs $\mathfrak{P}$ and partially order $\mathfrak{P}$ in the usual fashion, viz:

$$<S, \lambda> \leqq <T, \mu> \iff (1)\ T \subseteq S \quad \text{and (2) the diagram}$$



commutes (i.e., $\lambda(x) = S\mu(x)$).

Now $\mathfrak{P} \neq \emptyset$ as $<N, \mathrm{id}> \in \mathfrak{P}$. If $<S_\alpha, \lambda_\alpha>$ is a totally ordered subfamily of $\mathfrak{P}$, let $S = \bigcap_\alpha S_\alpha$. By Lemma 1, $G/S = \operatorname{proj\,lim}_\alpha G/S_\alpha$; so, as $\lambda_\beta(x) \to \lambda_\alpha(x)$ for $\beta \geqq \alpha$ under the map $G/S_\beta \to G/S_\alpha$, we see that for each $x \in G/N$, the family $\{\lambda_\alpha(x)\}$ represents a point $\lambda(x) \in G/S$. Clearly, $<S, \lambda>$ belongs to $\mathfrak{P}$, and we have proved $\mathfrak{P}$ is inductive.

By Zorn's lemma, there exists a maximal pair $<S, \lambda>$ in $\mathfrak{P}$. It is only necessary to prove that $S = \{1\}$. Were $S \neq \{1\}$, there would exist an open normal subgroup U of G with $S \not\subseteq U$. Therefore, $S \cap U < S$. We shall construct the section $G/S \to G/S \cap U$, and this will yield the desired contradiction.

Let $\underline{G} = G/S \cap U$, $\underline{S} = S/S \cap U$, then G/S is $\underline{G}/\underline{S}$ and our problem is to construct the section $\underline{G}/\underline{S} \to \underline{G}$ for the profinite group $\underline{G}$. But $\underline{S}$ is isomorphic to SU/U which is *finite* (being contained in G/U). Hence, our problem is reduced to the case of a finite normal subgroup. As $\underline{S}$ is finite, there is an open normal subgroup $\underline{V}$ of $\underline{G}$ such that $\underline{S} \cap \underline{V} = \{1\}$. The projection $\underline{G} \to \underline{G}/\underline{S}$ when restricted to $\underline{V}$ is a monomorphism. Since all groups are compact Hausdorff, $\underline{V}$ is topologically isomorphic to its image in $\underline{G}/\underline{S}$. The inverse map of this isomorphism is a continuous map from an *open* subgroup of $\underline{G}/\underline{S}$ onto an open subgroup of $\underline{G}$. Now a translation of this mapping to the finitely many cosets in $\underline{G}/\underline{S}$ yields our section $\underline{G}/\underline{S} \to \underline{G}$. Q.E.D.

COROLLARY. *If* M, N *are closed, normal subgroups of the profinite group* G, *with* $N \supseteq M$, *then there exists a section* $G/N \to G/M$.

Remark. One of the features of the theory of profinite groups which makes it important for various problems in number theory and geometry is that, in large measure, many mapping properties and number-theoretic properties of finite groups are (when attention is paid to their proper formulation) in reality valid for the larger class of profinite groups. An example is the cross-section theorem above; others follow in the next section.

§2. Supernatural numbers and the Sylow Theory.

DEFINITION 2. *A supernatural number* is a formal product

$$\prod_p p^{n_p}$$

where the product is taken over *all* prime numbers and n_p is an integer $0 \leqq n_p \leqq \infty$ (observe: ∞ is allowed!).

The theory of such numbers is entirely multiplicative, and it is easy to define the product, l.c.m. and g.c.d. of supernatural numbers or s-numbers as we shall call them. The connection with profinite groups is essentially given in the following definition.

DEFINITION 3. Let G be a profinite group, H a closed subgroup. By the *index of* H *in* G, we mean the s-number given by

$$(G:H) = \text{l.c.m.}(G/U : H/H \cap U) \text{ as } U \text{ ranges over all open normal subgroups of } G.$$

The *order of* G is defined by the equation

$$|G| = (G:1) = \text{l.c.m.}_U |G/U| \ .$$

Exercise. $(G:H) = \text{l.c.m.}(G:U)$ over those open, normal U with $H \subseteq U$.

If s is an s-number, then s is a p-*power* (*prime–to–*p) $\Longleftrightarrow$ $n_q = 0$ for all $q \neq p$ ($n_p = 0$). G is a p-*group* $\Longleftrightarrow$ $|G|$ is a p-power.

The first indication that things are all right is

PROPOSITION 1. (Lagrange's Theorem). *Let* $S \supseteq K$ *be closed subgroups of a profinite group* G. *Then*

$$(G:K) = (G:S)(S:K)$$

Proof: $(G:K) = \underset{\alpha}{\text{l.c.m.}}\,(G/U_\alpha : K/K \cap U_\alpha)$, where the U_α range over all open, normal subgroups of G. Now $K/K \cap U_\alpha = KU_\alpha/U_\alpha$ and $SU_\alpha \supseteq KU_\alpha$. Hence,

$$(G/U_\alpha : K/K \cap U_\alpha) = (G/U_\alpha : SU_\alpha/U_\alpha)(SU_\alpha/U_\alpha : KU_\alpha/U_\alpha)$$

$$= (G:SU_\alpha)(S/S \cap U_\alpha : K/K \cap U_\alpha) \ .$$

However, $S \cap U_\alpha = S_\alpha$ is open, normal in S, and the family of such is final in the set of all open, normal subgroups of S. Therefore,

$$(G/U_\alpha : K/K \cap U_\alpha) = (G:SU_\alpha)(S/S_\alpha : K/K \cap S_\alpha) \ .$$

It is easy to see (but requires a small separate argument which is left to the reader) that

$$(G:K) = \underset{\alpha}{\text{l.c.m.}}(G:SU_\alpha)\ \underset{\alpha}{\text{l.c.m.}}(S/S_\alpha : K/K \cap S_\alpha) \ ;$$

hence, $(G:K) = (G:S)(S:K)$. Q.E.D.

A p-*Sylow group* S of a profinite group G is a closed sub-p-group such that $(G:S)$ is prime–to–p.

THEOREM 4. (Sylow Theorem for Profinite Groups). *Let* G *be a profinite group, and let* p *be a prime number. Then*

(1) G *possesses* p-*Sylow subgroups;*

(2) *If* T *is any* p-*subgroup of* G *then* T *is contained in some* p-*Sylow subgroup of* G.

(3) *Any two* p-*Sylow subgroups of* G *are conjugate in* G.

Proof: We shall give two proofs of part (1) of this theorem. The first is due to John Tate, the second to J.-P. Serre. For the first, we let $\mathfrak{S}$ be the set of all subgroups $H \subseteq G$ such that $(G:H)$ is prime-to-p. Since $G \in \mathfrak{S}$, $\mathfrak{S}$ is non-empty and we partially order it by inclusion. If $\{H_\alpha\}$ is a chain in $\mathfrak{S}$, let $H = \bigcap_\alpha H_\alpha$. Let U be open, normal in G, then $HU \supseteq H$ and is open in G. Because the H_α are compact, there exists an index α for which $H_\alpha \subseteq HU$. Thus $(G:HU)$ divides $(G:H_\alpha)$; hence, $(G:HU)$ is prime-to-p. It follows that $H \in \mathfrak{S}$; whence, $\mathfrak{S}$ is inductive. Choose a minimal element, P, of $\mathfrak{S}$. I claim $|P|$ is a p-power. If not, there would exist an open, normal subgroup U of G with $(P:P \cap U)$ not a p-power. As $P/P \cap U$ is finite, it possesses a p-Sylow subgroup $Q/P \cap U$, with $P \neq Q$. But then, $(P:Q)$ is prime-to-p, and Q is smaller than P in $\mathfrak{S}$, a contradiction.

The second (Serre's) proof of (1) uses the following well-known fact: *The projective limit of a non-empty family of* finite *sets is non-empty.* This being said, let $\{U_\alpha\}$ be the family of all open, normal subgroups of G, and let $P(U_\alpha)$ be the set of all p-Sylow subgroups of G/U_α. By the ordinary Sylow Theorem, the sets $P(U_\alpha)$ are non-empty and finite. Moreover, if $\beta \geq \alpha$, then $U_\beta \subseteq U_\alpha$, so the surjection $G/U_\beta \to G/U_\alpha$ yields a map $P(U_\beta) \to P(U_\alpha)$. By our remark, there exists an element $\mathfrak{P}$ in $\operatorname{proj\,lim}_\alpha P(U_\alpha)$. What is such a $\mathfrak{P}$? It is a family P_α of subgroups of G/U_α such that each P_α is a p-Sylow subgroup of G/U_α and such that for $\beta \geq \alpha$, $P_\beta \to P_\alpha$ exists and is consistent for $\gamma \geq \beta \geq \alpha$, In other words, $\mathfrak{P}$ is a projective mapping family of p-Sylow sugroups from G/U_α, for each α. Let $P = \operatorname{proj\,lim}_\alpha P_\alpha$, then P is a p-group. I claim $(G:P)$ is prime-to-p. But,

$$(G:P) = \text{l.c.m.}(G/U_\alpha : P/P \cap U_\alpha) = \text{l.c.m.}(G/U_\alpha : P_\alpha)$$

$$= \text{prime-to-p}\,.$$

Finally, to prove (2) and (3) it suffices to prove: *If* T *is a* p-*subgroup*

of G, *there is some* $\sigma \in G$ *with* $T^{\sigma} \subseteq P$, *where* P *is a given* p-*Sylow subgroup of* G. Here, the notation T^{σ} means $\sigma^{-1} T\sigma$. Choose any open normal subgroup U of G, and consider TU and PU. We know that PU/U is a p-Sylow subgroup of G/U, so by finite Sylow Theory, there exists a $\bar{\sigma}_U$ in G/U with

$$(*) \qquad (TU/U)^{\bar{\sigma}_U} \subseteq (PU/U) \ .$$

Let R_U be the set of all σ_U in G such that $\bar{\sigma}_U$ satisfies (*) above. Then (1) $R_U \neq \emptyset$ for any U, (2) R_U is a union of cosets of U in G so is closed in G, and (3) the sets R_U have the finite intersection property. (The last assertion follows from $R_V \subseteq R_U$ if $V \subseteq U$.) By the compactness of G, the intersection $\bigcap_U R_U$ is non-empty; and it is clear that $\sigma \in \bigcap_U R_U$ is the required element of G. Q.E.D.

Examples. (4) If G is a group generated by a set $\{x_\alpha\}$ of elements, let $\mathcal{S}$ be the set of all normal subgroups U of G such that (a) G/U is finite, (b) almost all x_α lie in U. Let $\hat{G} = \underset{U}{\text{proj lim}}\ G/U$, then $\hat{G}$ is called the *profinite completion of* G. For example if G is $\mathbf{Z}$ we get $\hat{\mathbf{Z}}$ as in example (2P).

(5) Let G = F(X) be the free-group on X. Its profinite completion is called the *free-profinite group on* X. If we restrict attention to those subgroups U for which in addition (c) (G: U) is a p-power, then we get $F_p(X)$ (or in example (4) $\hat{G}_p$) which is called the *free-profinite* p-*group on* X (or the p-*profinite completion* of G). If X is the set with one element, we have $F(X) = \mathbf{Z}$, $F_p(X) = \mathbf{Z}_p$ = p-adic integers (see example (2P)) = p-Sylow subgroup of $\hat{\mathbf{Z}}$.

CHAPTER II

COHOMOLOGY OF PROFINITE GROUPS

§1. δ-functors and the definition of the cohomology of profinite groups.

Let $\mathfrak{A}$ be an abelian category (think of modules over a ring, or abelian groups on which some group acts *via* automorphisms), then we have the notion of an exact sequence of objects of $\mathfrak{A}$

$$A' \xrightarrow[\psi]{} A \xrightarrow[\phi]{} A''$$

This means $\ker \phi = \operatorname{Im} \psi$; and to say that

$$0 \longrightarrow A' \xrightarrow[\psi]{} A \xrightarrow[\phi]{} A'' \longrightarrow 0 \tag{1}$$

is exact means that ψ is injective, ϕ is surjective, and $\ker \phi = \operatorname{Im} \psi$. An exact sequence as in (1) is called a *short exact sequence.*

Suppose we have a family of functors $T^0, T^1, T^2, \ldots$, from $\mathfrak{A}$ to the category of abelian groups. This family of functors is called a δ-*functor* (or *exact, connected sequence of functors*) iff

(1) For all short exact sequences as above and for all $n \geq 0$, there exists a homomorphism $\delta_n : T^n(A'') \to T^{n+1}(A')$ so that the long sequence obtained by using the δ_n, viz:

$$0 \to T^0(A') \to T^0(A) \to T^0(A'') \xrightarrow{\delta_0} T^1(A') \to T^1(A) \to T^1(A'') \to$$

$$T^2(A') \to T^2(A) \to \cdots$$

is *exact* (in particular, we assume T^0 is left-exact!), and