Travaux mathématiques, Volume 22 (2013), 179–230, © by the author

Introduction to Profinite Groups

by Luis Ribes

Abstract

This is the content of three lectures at the Winter School on Galois Theory in Luxembourg, February 2012. They cover basic properties of profinite groups, emphasizing the connection with Galois Theory, and including free profinite groups, free product, module theory and cohomology. The material is reasonably self-contained with either complete proofs or full references.

MSC (2010): 20E18, 11S20, 11S25.

Preface

These notes follow very closely the content of my three lectures at the Winter School on Galois Theory in Luxembourg, 15 - 24 February 2012. The invitation from the organizers of the meeting, Sara Arias-de-Reyna, Lior Bary-Soroker and Gabor Wiese, came with the challenge of covering the vast subject of Profinite Groups in a few hours and for an audience with different levels of knowledge of the subject. My intent was to present an overview of profinite groups, with emphasis on the main concepts and properties, and connections with Galois Theory. The notes touch on many topics covered with different level of detail. In some cases full proofs are included, and for the rest precise statements are given with sketched proofs sometimes and references for complete proofs for all the results. There are several sources where one can find detailed proofs and expand on the material covered in these lectures, and we list some of them in the References.

Contents

1 Lecture 1

1.1 Infinite Galois extensions

Let K be a field and N a Galois extension of K (i.e. algebraic, normal and separable). Let

$$G = G_{N/K} = \{\sigma \in \mathrm{Aut}(N) \bigm| \sigma_{|K} = \mathrm{id}_K\}$$

be the Galois group of this extension. Denote by $\{N : K\}$ and $\{G : 1\}$ the lattices of intermediate fields L, $K \subseteq L \subseteq N$, and subgroups $H \subseteq G$, respectively. Then there are maps

$$\{N : K\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{G : 1\}$$

defined by

$$\begin{aligned} \Phi(L) &= \{\sigma \in G_{N/K} \bigm| \sigma_{|L} = \mathrm{id}_L\} = G_{N/L} \quad (K \subseteq L \subseteq N) \\ \Psi(H) &= \{x \in N \bigm| Hx = x\} \quad (H \leq G), \end{aligned}$$

which reverse inclusion, i.e., they are anti-homomorphisms of lattices.

The main theorem of Galois theory for finite extensions can be stated then as follows.

Theorem 1.1. *Let N/K be a finite Galois extension. Then*

(a) $[N : K] = \#G_{N/K}$*;*

(b) *The maps Φ and Ψ are inverse to each other, i.e, they are anti-isomorphisms of lattices.*

(c) *If $L \in \{N : K\}$ and $\Phi(L) = G_{N/L}$, then L is normal over K iff $G_{N/L}$ is a normal subgroup of G, in which case $G_{L|K} \cong G_{N/K}/G_{N/L}$.*

Let us assume now that the Galois extension N/K is not necessarily finite. The one still has the following

Proposition 1.2. $\Psi\circ\Phi = \mathrm{id}_{\{N:K\}}$. *In particular Φ is injective and Ψ is surjective.*

Proof. If $K \subseteq L \subseteq N$ one certainly has

$$\Psi(\Phi(L)) = \Psi(G_{N/L}) = \{x \in N \bigm| G_{N/L}x = x\} \supset L.$$

On the other hand, if $x \in N$ and $G_{N/L}x = x$, then x is the only conjugate of x, i.e. $x \in L$. □

However in the general case Φ and Ψ are not anti-isomorphisms; in other words in the infinite case it could happen that different subgroups of $G_{N/K}$ have the same fixed field, as the following example shows.

Example 1.3. Let p be a prime and let $K = \mathbf{F}_p$ be the field with p elements. Let $\ell \neq 2$ be a prime number, and consider the sequence

$$K = K_0 \subset K_0 \subset \cdots ,$$

where K_i is the unique extension of K of degree $[K_i : K] = \ell^i$. Let

$$N = \bigcup_{i=1}^{\infty} K_i;$$

then

$$K_i = \{x \in N \mid x^{p^{\ell^i}} - x = 0\}.$$

Let $G = G_{N/K}$. Consider the Frobenius K-automorphism

$$\varphi \colon N \longrightarrow N$$

defined by $\varphi(x) = x^p$. Set

$$H = \{\varphi^n \mid n \in \mathbf{Z}\}.$$

We shall prove that (a) H and G have the same fixed field, i.e., $\Psi(G) = \Psi(H)$, and (b) $H \neq G$, establishing that Ψ is not injective.

For (a): It suffices to show that $\Psi(H) = K$. Let $x \in N$ with $Hx = x$; then $\varphi(x) = x$; so $x^p = x$; hence $x \in K$.

For (b): We construct a K-automorphism σ of N, which is not in H, in the following way. For each $i = 1, 2 \ldots$, let $k_i = 1 + \ell + \cdots + \ell^{i-1}$, and consider the K-automorphisms φ^{k_i} of N. Since

$$\varphi^{k_{i+1}}_{|K_i} = \varphi^{k_i}_{|K_i},$$

we can define a K-automorphism

$$\sigma \colon N \longrightarrow N$$

by setting

$$\sigma(x) = \varphi^{k_i}(x), \qquad \text{when } x \in K_i.$$

Now, if $\sigma \in H$, say $\sigma = \varphi^n$ we would have for each $i = 1, 2 \ldots$

$$\sigma_{|K_i} = \varphi^n_{|K_i} = \varphi^{k_i}_{|K_i},$$

and hence

$$n \equiv k_i \pmod{\ell^i}$$

for each i, since $G_{K_i/K}$ is the cyclic group generated by $\varphi_{|K_i}$. Multiplying this by $(\ell - 1)$ we would obtain $(\ell - 1)n \equiv -1 \pmod{\ell^i}$, for each i, which is impossible if $\ell \neq 2$.

Remark 1.4. The key idea in the above example is the following: what happens is that the Galois group $G_N = G_{N/\mathbf{F}_p}$ is isomorphic to the additive group $\mathbf{Z}_\ell$ of the ℓ-adic integers. The Frobenius automorphism φ corresponds to $1 \in \mathbf{Z}_\ell$, so that the group H is carried onto $\mathbf{Z} \subseteq \mathbf{Z}_\ell$. The elements of G which are not in H correspond to the ℓ-adic integers which are not in $\mathbf{Z}$ (for instance, in our case $\sigma = 1 + \ell + \ell^2 + \ell^3 + \cdots$).

1.2 The Krull topology

Although the above example shows that Theorem 1.1 does not hold for infinite Galois extension, it suggest a way of modifying the theorem so that it will in fact be valid even in those cases. The map σ of the example is in a sense approximated by the maps φ^{k_i}, since it coincides with φ^{k_i} on the subextension K_i which becomes larger and larger with increasing i, and $N = \bigcup_{i=1}^{\infty} K_i$. This leads to the idea of defining a topology in G so that in fact $\sigma = \lim \varphi^{k_i}$. Then σ would be in the closure of H and one could hope that G is the closure of H, suggesting a correspondence of the intermediate fields of N/K and the closed subgroups of G. In fact this is the case as we will see.

Definition 1.5. Let N/K be a Galois extension and $G = G_{N/K}$. The set

$$\mathcal{S} = \{G_{N/L} \mid L/K \text{ finite, normal extension, } L \in \{N : K\}\}$$

determines a basis of open neighbourhoods of $1 \in G$. The topology defined by $\mathcal{S}$ is called the 'Krull topology' of G.

Remark.

1. If N/K is a finite Galois extension, the the Krull topology of $G_{N/K}$ is the discrete topology.

2. Let $\tau, \sigma \in G_{N/K}$. Then $\tau \in \sigma G_{N/L} \iff \sigma^{-1}\tau \in G_{N/L} \iff \sigma_{|L} = \tau_{|L}$, i.e., two elements of $G_{N/K}$ "are near" if they coincide on a large field L.

Proposition 1.6. *Let N/K be a Galois extension and let $G = G_{N/K}$. Then G endowed with the Krull topology is a (i) Hausdorff, (ii) compact, and (iii) totally-disconnected topological group.*

Proof.

For (i): Let $\mathcal{F}_n$ denote the set of all finite, normal subextension L/K of N/K. We have

$$\bigcap_{U \in \mathcal{S}} U = \bigcap_{L/K \in \mathcal{F}_n} G_{N/L} = 1,$$

since

$$N = \bigcup_{L/K \in \mathcal{F}_n} L.$$

Then, $\sigma, \tau \in G$, $\sigma \neq \tau \Rightarrow \sigma^{-1}\tau \neq 1 \Rightarrow \exists U_0 \in \mathcal{S}$ such that $\sigma^{-1}\tau \notin U_0 \Rightarrow \tau \notin \sigma U_0 \Rightarrow \tau U_0 \cap \sigma U_0 = \emptyset$.

For (ii): Consider the homomorphism

$$h\colon G \to \prod_{L/K \in \mathcal{F}_n} G_{L/K} = P,$$

defined by

$$h(\sigma) = \prod_{L/K \in \mathcal{F}_n} \sigma_{|L}.$$

(Notice that P is compact since every $G_{L/K}$ is a discrete finite group.)

We shall show that h is an injective continuous mapping, that $h(G)$ is closed in P and that h is an open map into $h(G)$. This will prove that G is homeomorphic to the compact space $h(G)$.

Let $\sigma \in G$ with $h(\sigma) = 1$; then $\sigma_{|L} = 1$, since $N = \bigcup_{L/K \in \mathcal{F}_n} L$. Thus h is injective.

To see that h is continuous consider the composition

$$G \xrightarrow{h} P \xrightarrow{g_{L/K}} G_{L/K}$$

where $g_{L/K}$ is the canonical projection. It suffices to show that each $g_{L/K}h$ is continuous; but this is clear since

$$(g_{L/K}h)^{-1}(\{1\}) = G_{N/L} \in \mathcal{S}.$$

To prove that $h(G)$ is closed consider the sets $M_{L_1/L_2} = \{p\sigma_L \in P \mid (\sigma_{L_1})_{|L_2} = \sigma_{L_2}\}$ defined for each pair $L_1/K, L_2/K \in \mathcal{F}_n$ with $N \supseteq L_1 \supseteq L_2 \supseteq K$. Notice that M_{L_1/L_2} is closed in P since it is a finite union of closed subsets, namely, if $G_{L_2/K} = \{f_1, f_2, \dots, f_r\}$ and S_i is the set of extensions of f_i to L_1, then

$$M_{L_1/L_2} = \bigcup_{i=1}^{r} \Big(\prod_{\substack{L \neq L_1, L_2 \\ L/K \in \mathcal{F}_n}} G_{L/K} \times S_i \times \{f_i\} \Big).$$

On the other hand

$$h(G) \subseteq \bigcap_{L_1 \supseteq L_2} M_{L_1/L_2};$$

and if

$$\prod_{L/K \in \mathcal{F}_n} \sigma_L \in \bigcap_{L_1 \supseteq L_2} M_{L_1/L_2}$$

we can define a K-automorphism $\sigma\colon N \to N$ by $\sigma(x) = \sigma_L(x)$ if $x \in L$; so that $h(\sigma) = \prod_{L/K \in \mathcal{F}_n} \sigma_L$. I.e.,

$$h(G) = \bigcap_{L_1 \supseteq L_2} M_{L_1/L_2},$$

and hence $h(G)$ is closed.

Finally h, as a map into $h(G)$, is open; indeed, if $L/K \in \mathcal{F}_n$,

$$h(G_{N/L}) = h(G) \cap \big(\prod_{\substack{L' \neq L \\ L'/K \in \mathcal{F}_n}} G_{L'/K} \times \{1\} \big)$$

which is open in $h(G)$.

For (iii): It is enough to prove that the connected component H of 1 is $\{1\}$. For each $U \in \mathcal{S}$ let $U_H = U \cap H$; then U_H is nonempty and it is open in H.

Let

$$V_H = \bigcup_{\substack{x \in H \\ a \notin U_H}} xU_H;$$

then V_H is open in H, $U_H \cap V_H = \emptyset$ and $H = U_H \cap V_H$. Hence $V_H = \emptyset$; i.e., $U \cap H = H$ for each $U \in \mathcal{S}$. Therefore

$$H \subseteq \bigcap_{U \in \mathcal{S}} U = \{1\},$$

so $H = \{1\}$. □

Proposition 1.7. *Let N/K be a Galois extension. The open subgroups of $G = G_{N/K}$ are just the groups $G_{N/L}$, where L/K is a finite subextension of N/K. The closed subgroups are precisely the intersections of open subgroups.*

Proof. Let L/K be a finite subextension of N/K. Choose a finite normal extension $\tilde{L}$ of K such that $N \supseteq \tilde{L} \supseteq L \supseteq K$. Then

$$G_{N/\tilde{L}} \leq G_{N/L} \leq G;$$

so

$$G_{N/L} = \bigcup_{\sigma \in G_{N/L}} \sigma G_{N/\tilde{L}};$$

i.e., $G_{N/L}$ is the union of open sets and thus open. Conversely, let H be an open subgroup of G; then there exists a finite normal extension $\tilde{L}$ with

$$G_{N/\tilde{L}} \leq H \leq G.$$

Consider the epimorphism

$$G \to G_{\tilde{L}/K}$$

defined by restriction. Its kernel is $G_{N/\tilde{L}}$. The image of H under this map must be of the form $G_{\tilde{L}/L}$, for some field L with $\tilde{L} \supseteq L \supseteq K$, since $G_{\tilde{L}/K}$ is the Galois group of a finite Galois extension. Thus

$$H = \{\sigma \in G \mid \sigma_{|L} = \mathrm{id}_L\} = G_{N/L}.$$

Since open subgroups are closed, so is their intersection. Conversely, suppose H is a closed subgroup of G; clearly

$$H \subseteq \bigcap_{U \in \mathcal{S}} HU.$$

On the other hand, let $\sigma \in \bigcap_{U \in \mathcal{S}} HU$; then for every $U \in \mathcal{S}$, one has $\sigma U \cap H \neq \emptyset$; so every neighborhood of σ meets H; hence $\sigma \in H$. Thus H is the intersection of the open subgroups HU of H, $(U \in \mathcal{S})$. □

We are now in a position to generalize Theorem 1.1 to infinite Galois extensions.

Theorem 1.8 (Krull)**.** *Let N/K be a (finite or infinite) Galois extension and let $G = G_{N/K}$. Let $\{N : K\}$ be the lattice of intermediate fields $N \supseteq L \supseteq K$, and let $\{G : 1\}$ be the lattice of closed subgroups of G. If $L \in \{N : K\}$ define*

$$\Phi(L) = \{\sigma \in G \mid \sigma_{|L} = \mathrm{id}_L\} = G_{N/L}.$$

Then Φ is a lattice anti-isomorphism of $\{N : K\}$ to $\{G : 1\}$. Moreover $L \in \{N : K\}$ is a normal extension of K iff $\Phi(L)$ is a normal subgroup of G; and if this is the case, $G_{L/K} \cong G/\Phi(L)$.

Proof. Since $\Phi(L) = G_{N/L}$ is compact (Prop. 1.6), it is closed in G; so Φ is in fact a map into $\{G : 1\}$. Define

$$\Psi \colon \{G : 1\} \to \{N : K\}$$

by

$$\Psi(H) = \{x \in N \mid Hx = x\}.$$

Clearly Proposition 1.2 is still valid and we have $\Psi \circ \Phi = \mathrm{id}_{\{N:K\}}$. Now we prove that $\Phi \circ \Psi = \mathrm{id}_{\{G:1\}}$. If L/K is finite,

$$\Phi(\Psi(G_{N/L})) = \Phi(\Psi(\Phi(L))) = \Phi(L) = G_{N/L}.$$

If $H \in \{G : 1\}$, then, by Proposition 1.7,

$$H = \bigcap G_{N/L},$$

the intersection running through the collection of extensions N/L with L/K finite. Then

$$\begin{aligned}\Phi(\Psi(H)) = \Phi(\Psi(\bigcap G_{N/L})) &= (\Phi\Psi)(\bigcap \Phi(L))) \\ &= (\Phi\Psi\Phi)(\bigcup L) = \Phi(\bigcup L) = \bigcap \Phi(L) = \bigcap G_{N/L} = H.\end{aligned}$$

Assume that L is a normal extension of K, and let $H = \Phi(L)$. Then $\sigma L = L$, for all $\sigma \in G$; but since $\sigma L = \Psi(\sigma H \sigma^{-1})$, this is equivalent to saying that $\sigma H \sigma^{-1} = H$, for all σ, i.e., that H is normal in G. Conversely, suppose that H is an invariant subgroup of G, and let $\Psi(H) = L$. So $\sigma L = L$, for all $\sigma \in G$, i.e., L is the fixed field of the group of restrictions of the $\sigma \in G$ to L. Thus L/K is Galois and hence normal. Finally, since every K-automorphism of L can be extended to a K-automorphism of N, the homomorphism

$$G \to G_{L/K},$$

given by restriction, is onto. The kernel of this homomorphism is $\Phi(L)$; thus $G_{L/K} \cong G/\Phi(L)$. □

1.3 Profinite Groups

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

$$\begin{tikzcd} X_i \arrow[rr, "\varphi_{ik}"] \arrow[dr, "\varphi_{ij}"'] & & X_k \\ & X_j \arrow[ur, "\varphi_{jk}"'] & \end{tikzcd}$$

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 denote such a system by $\{X_i, \varphi_{ij}, I\}$. The *inverse limit* or *projective limit*

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

of the inverse system $\{X_i, \varphi_{ij}, I\}$ is the subspace (respectively, subgroup) X 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 $i \succeq j$. We assume that X has the topology induced by the product topology of $\prod_{i\in I} X_i$. For each $i \in I$, 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 $\varphi_{ij}\varphi_i = \varphi_j$ $(j \prec i)$. The space (respectively, topological group) X together with the maps (respectively, homomorphisms) φ_i satisfy the following universal property that in fact **characterizes** (as one easily checks) the inverse limit:

Proposition 1.9 (Universal property of inverse limits)**.** *Suppose Y is another topological space (respectively, group) and $\psi_i : Y \to X_i$ $(i \in I)$ are continuous maps (respectively, continuous homomorphisms) such that $\varphi_{ij}\psi_i = \psi_j$ $(j \prec i)$. Then there exists a unique continuous map (respectively, continuous homomorphism) $\psi : Y \to X$ such that for each $i \in I$ the following diagram*

$$\begin{tikzcd} Y \arrow[r, dotted, "\psi"] \arrow[dr, "\psi_i"'] & X \arrow[d, "\varphi_i"] \\ & X_i \end{tikzcd}$$

commutes.

Let $\mathcal{C}$ denote a nonempty collection of (isomorphism classes of) finite groups closed under taking subgroups, homomorphic images and finite direct products (sometimes we refer to $\mathcal{C}$ as a *variety of finite groups* or a *pseudovariety of finite groups*). If in addition one assumes that, whenever $A, B \in \mathcal{C}$ and $1 \to A \to G \to B \to 1$ is an exact sequence of groups, then $G \in \mathcal{C}$, we say that $\mathcal{C}$ is an *extension-closed variety of finite groups* . For example

(i) the collection of all finite groups;

(ii) the collection of all finite p-groups (for a fixed prime p);

(iii) the collection of all finite nilpotent groups.

Note that (i) and (ii) are extension-closed varieties of finite groups, but (iii) is a variety of finite groups which is not extension-closed.

Let $\mathcal{C}$ be a variety of finite groups; and let $\{G_i, \varphi_{ij}, I\}$ be an inverse system of groups in $\mathcal{C}$ over a directed poset I; then we say that

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

is a *pro-$\mathcal{C}$ group*. If $\mathcal{C}$ is an in (i), (ii) or (iii) above, we say that then G is, respectively, a *profinite group*, *pro-p group* or a *pronilpotent group*.

Example 1.10 (Examples of Profinite Groups)**.**

(a) The Galois group $G_{N/K}$ of a Galois extension N/K of fields (see Proposition 1.6 above and Theorem 1.12 below).

(b) Let G be a group. Consider the collection

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

Make $\mathcal{N}$ into a directed poset by defining $M \preceq N$, if $M \geq N$ $(M, N \in \mathcal{N})$. 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. 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.

(c) As a special case of (b), 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*.

Lemma 1.11. *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

$$\Big(\prod_{i \neq i_1, \dots, i_t} G_i \Big) \times \{1\}_{i_1} \times \cdots \times \{1\}_{i_t},$$

for any finite collection of indexes $i_1, \dots, i_t \in I$, 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 $i_0 \succeq i_1, \dots, i_t$. Then

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

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

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

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

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

□

Theorem 1.12 (Topological characterizations of pro-$\mathcal{C}$ groups)**.** *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) *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*

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

For a formal proof of this theorem, see [5], Theorem 2.1.3. For properties of compact totally disconnected topological spaces, see Chapter 1 of [5].

1.4 Basic Properties of Profinite Groups

Notation. If G is topological group, we write $H \leq_o G$ (respectively, $H \leq_c G$) to indicate that H is an open (respectively, closed) subgroup of G

Lemma 1.13. (a) *Let G be a pro-$\mathcal{C}$ group. An open subgroup of G is also closed. If H is a closed subgroup of G, then H is the intersection of all the open subgroups U containing H.*

(b) *Let G be a pro-$\mathcal{C}$ group. If H be a closed subgroup of G, then H is a pro-$\mathcal{C}$ group. If K is a closed normal subgroup of G, then G/K is a pro-$\mathcal{C}$ group.*

(c) *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.*

The proof of this lemma is an easy exercise using the characterizations in Theorem 1.12. For a formal proof of this theorem, see [5], Propositions 2.1.4 and 2.2.1.

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 1.14. *Let $K \leq H$ be closed subgroups of a profinite group G . Then there exists a continuous section*

$$\sigma \colon G/H \longrightarrow G/K,$$

of the natural projection $\pi : G/K \longrightarrow G/H$, such that $\sigma(1H) = 1K$.

Proof. We consider two cases.

- *Case 1.* Assume that K has finite index in H. Then K is open in H, and therefore there exists an open normal subgroup U of G with $U \cap H \leq K$. Let $x_1 = 1, x_2, \dots, x_n$ be representatives of the distinct cosets of UH in G. Then G/H is the disjoint union of the spaces x_iUH/H, $i = 1, 2, \dots, n$. We will prove that the maps

  $$\pi_i \colon x_iUK/K \to x_iUH/H$$

  $i = 1, 2, \dots, n$, defined as restrictions of π, are homeomorphisms. Then it will follow that $\sigma = \bigcup_{i=1}^n \pi_i^{-1}$ will be the desired section. It is plain that π_i is a continuous surjection. On the other hand if $\pi_i(x_iu_1) = \pi_i(x_iu_2)$,

$(u_1, u_2 \in U)$, then $x_i u_1 u_2^{-1} x_i^{-1} \in H$. But since U is normal, $x_i u_1 u_2^{-1} x_i^{-1} \in U$, and hence $x_i u_1 u_2^{-1} x_i^{-1} \in H \cap U \leq K$. Thus $x_i u_1$ and $x_i u_2$ represent the same element in $x_i UK$, i.e., π is injective. Since $x_i UK$ is compact, π must be a homeomorphism.

- *Case 2.* General case. Let $\mathcal{T}$ be the set of pairs (T, t) where T is a closed subgroup of H with $K \leq T \leq H$, and $t\colon G/H \to G/T$ is a continuous section. Define a partial order in $\mathcal{T}$ by $(T, t) \geq (T', t') \iff T \leq T'$ and the diagram

$$\begin{tikzcd}
G/H \arrow[r, "t"] \arrow[dr, "t'"'] & G/T \arrow[d, "p"] \\
 & G/T'
\end{tikzcd}$$

commutes, where p is the canonical projection. Then $\mathcal{T}$ is inductively ordered. For assume $\{(T_\alpha, t_\alpha) \mid \alpha \in A\}$ is a totally ordered subset of $\mathcal{T}$, and let $T = \bigcap_{\alpha \in A} T_\alpha$. The surjections $G/T \to G/T_\alpha$ induce a surjective (since G/T is compact) continuous map

$$\varphi\colon G/T \to \varprojlim_{\alpha} G/T_\alpha,$$

which is also injective, for

$$\begin{aligned}
&x, y \in G, \quad \varphi x = \varphi y \Rightarrow x T_\alpha = y T_\alpha, \quad \forall \alpha \in A \Rightarrow \\
&x^{-1} y \in T_\alpha, \quad \forall \alpha \in A \Rightarrow x^{-1} y \in \bigcap_{\alpha} T_\alpha = T.
\end{aligned}$$

Therefore φ is a homeomorphism, since G/T is compact. The sections t_α define a continuous map

$$t\colon G/H \to G/T$$

which is easily seen to be a section. Moreover, we obviously have $(T, t) \geq (T_\alpha, t_\alpha)$, $\forall \alpha \in A$. Hence $\mathcal{T}$ is inductive. By Zorn's lemma there is a maximal element in $\mathcal{T}$, say $(\bar{T}, \bar{t})$. Then

$$K \leq \bar{T} \leq H \leq G.$$

We will show that $\bar{T}$ is contained in every open subgroup U containing K. This will imply $\bar{T} = K$. Consider an open subgroup $H \leq U \leq K$. Let $S = \bar{T} \cap U$; Then $S \leq \bar{T}$ and $[\bar{T} : S] < \infty$. Hence by Case 1, there is a section

$$t'\colon G/\bar{T} \to G/S,$$

and clearly $(S, t' \circ \bar{t}) \in \mathcal{T}$ with $(S, t' \circ \bar{t}) \geq (\bar{T}, \bar{t})$. So $S = \bar{T}$, and thus $\bar{T} \leq U$.

□

1.5 Profinite groups as Galois groups

Together with Theorem 1.8, the following result provides a new characterization of profinite groups.

Theorem 1.15 (Leptin)**.** *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 $\{t_i \in G/U_i \mid i = 1, \ldots, n\}$, 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 1.8; 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 1.8 that $G = H$. □

1.6 Supernatural numbers and Sylow subgroups

For a finite group, its 'order' is the cardinality of its underlying set; for finite groups the notion of cardinality provides fundamental information for the group as it is well known. However the cardinality of a profinite group G does not carry with it much information about the group. One can show that a nonfinite profinite group is necessarily uncountable (cf. [[5], Proposition 2.3.1]). Instead, there is a notion of 'order' $\#G$ of a profinite group G that we are explaining here which is useful: it provides information about the finite (continuous) quotients of G.

A *supernatural number* is a formal product

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

where p runs through the 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

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

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

- $\prod\limits_I n_i = \prod\limits_p p^{n(p)}$, where $n(p) = \sum\limits_i n(p,i)$;
- $\gcd\{n_i\}_{i \in I} = \prod\limits_p p^{n(p)}$, where $n(p) = \min\limits_i \{n(p,i)\}$;
- $\operatorname{lcm}\{n_i\}_{i \in I} = \prod\limits_p p^{n(p)}$, where $n(p) = \max\limits_i \{n(p,i)\}$.

(Here $\sum\limits_i n(p,i)$, $\min\limits_i \{n(p,i)\}$ and $\max\limits_i \{n(p,i)\}$ 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* 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 1.16. *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*

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

(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*

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

(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 (i.e., whenever H and K are in the family, there exists some subgroup L in the family with $L \leq H \cap K$). Assume that $H = \bigcap_{i\in I} H_i$. Then*

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

(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*

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

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

$$\#(\prod_{i\in I} G_i) = \prod_{i\in I} \#G_i;$$

(h) *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*

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

One can find a formal proof of these properties in [[5], Proposition 2.3.2].

If p is a prime number there is then a natural notion of *p-Sylow subgroup P* of a profinite group G: P is a pro-p group such that p does not divide $[G : P]$. Using the above notion of order for profinite groups, we can prove results analogous to the classical Sylow theorems for finite groups. To do this one uses as a basic tool the following property of compact Hausdorff spaces.

Proposition 1.17. *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, 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. □

Theorem 1.18. *Let p be a fixed prime number and let G be a profinite group. Then*

(a) *G contains a p-Sylow subgroup;*

(b) *Any pro-p subgroup of G is contained in a p-Sylow subgroup;*

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

Proof. Express G as

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

where $\{G_i, \varphi_{ij}, I\}$ is a surjective inverse system of finite groups (i.e., we assume that the all maps φ_{ij} of the inverse system are surjective).

(a) Let $\mathcal{H}_i$ be the set of all p-Sylow subgroups of G_i. Then $\mathcal{H}_i \neq \emptyset$. Since $\varphi_{ij} : G_i \to G_j$ 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 1.17,

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

Let $(H_i) \in \varprojlim \mathcal{H}_i$. Then H_i is a p-Sylow subgroup of G_i for each $i \in I$, and $\{H_i, \varphi_{ij}, I\}$ is an inverse system of finite groups. One easily checks that $H = \varprojlim H_i$ is a p-Sylow subgroup of G, as desired.

(b) Let H be a pro-p subgroup of G. Then, $\varphi_i(H)$ is a pro-p subgroup of G_i $(i \in I)$. Then there is some p-Sylow subgroup of G_i that contains $\varphi_i(H)$; so the set

$$\mathcal{S}_i = \{S \mid \varphi_i(H) \leq S \leq G_i \ , S \text{ is a } p\text{−Sylow subgroup of } G_i\}$$

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 p-Sylow subgroup of G.

(c) Let H and K be p-Sylow subgroups of G. Then $\varphi_i(H)$ and $\varphi_i(K)$ are p-Sylow subgroups of G_i $(i \in I)$, and so 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 1.6.2, let $q \in \varprojlim Q_i$. Then $q^{-1}Hq = K$, since $\varphi_i(q^{-1}Hq) = \varphi_i(K)$, for each $i \in I$.

□

2 Lecture 2

2.1 Generators of a profinite group

Let G be a profinite group and let X be a subset of G. We say that X *generates* G (as a profinite 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* 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.

Example. $\widehat{\mathbf{Z}}$ 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, and it is not procyclic.

Remark. If X is 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 2.1. *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 $\tilde{X}_i$. Then $\tilde{X}_K$ 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 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 $M = 1$. □

Notation Let G be a profinite group. Then $d(G)$ denotes the smallest cardinality of a set of generators of G converging to 1. $w_0(G)$ is the smallest cardinality of a fundamental system of neighbourhoods of 1.

Let X be a *profinite space* (=inverse limit of finite discrete spaces). Denote by $\rho(X)$ the the cardinal of the set of all clopen subsets of X.

Proposition 2.2. *Let G be an infinite profinite group.*

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

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

(c) *If $d(G)$ is infinite, $w_0(G) = d(G)$.*

Proof. See Section 2.6 in [5]. □

Proposition 2.3 (Hopfian property). *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. Then $\mathcal{U}_n$ 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 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. □

Proposition 2.4 (Gaschütz, Roquette)**.** *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 $H = \overline{\langle h_1, \dots, h_n \rangle}$. Then there exist $g_1, \dots, g_n \in G$ such that $G = \overline{\langle g_1, \dots, g_n \rangle}$ and $\varphi(g_i) = h_i$ $(i = 1, \dots, n)$.

Proof.

- *Case 1.* G is finite. For $\mathbf{h} = (h_1, \dots, h_n) \in H \times \cdots \times H$ with $\langle h_1, \dots, h_n \rangle = H$, let $t_G(\mathbf{h})$ denote the number of n-tuples

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

  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 1.17 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 $G = \overline{\langle g_1, \dots, g_n \rangle}$. □

The following results are characterizations of the value $w_0(G)$; they provide useful tools to prove results by transfinite induction. For proofs of these results can be found in [5], Theorem 2.6.4 and Corollary 2.6.6.

Theorem 2.5. *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 $\lambda \leq \mu$*

$$G = G_0 \geq G_1 \geq \cdots \geq G_\lambda \geq \cdots \geq G_\mu = 1 \tag{2.1}$$

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 (2.1) *can be chosen in such a way that*

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

Corollary 2.6. *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.*

2.2 Free pro-$\mathcal{C}$ groups

Definition 2.7. Let Y be a set and G a pro-$\mathcal{C}$ group. We say that a map $\rho\colon A \to G$ is *convergent to* 1 if every open normal subgroup of G contains a.e. (almost every, i.e. all but a finite number) $\rho(y)$, $y \in Y$.

Definition 2.8. A pro-$\mathcal{C}$ group F together with a map $\iota\colon Y \to F$ convergent to 1 is called a *free pro-$\mathcal{C}$ group* on the set Y if it satisfies following universal property: if $\varphi\colon Y \to G$ is any map convergent to 1 of Y into a pro-$\mathcal{C}$ group G, then there exists a unique continuous homomorphism $\bar{\varphi}\colon F \to G$ such that the diagram

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

commutes.

Proposition 2.9. *For every set Y there exists a unique free pro-$\mathcal{C}$ group on the set Y. It is denoted $F_{\mathcal{C}}(Y)$.*

Sketch. If $\iota\colon A \to F$ and $\iota'\colon A \to F'$ are free pro-$\mathcal{C}$ groups on Y, let $\psi\colon F \to F'$ and $\psi'\colon F' \to F$ be the unique continuous homomorphisms such that $\psi\iota = \iota'$ and $\psi'\iota' = \iota$. Then we must have $\psi' \circ \psi = \mathrm{id}_F$ and $\psi \circ \psi' = \mathrm{id}_{F'}$. Thus F and F' are isomorphic, and hence $F_{\mathcal{C}}(Y)$ is unique.

We shall construct $F_{\mathcal{C}}(Y)$ in the following manner. Let $\iota^0\colon Y \to \Phi$ be the abstract free group with basis Y and denote by $\mathcal{N}$ the system of all normal subgroups N of F such that

(1) $\Phi/N \in \mathcal{C}$, and

(2) N contains a.e. $\iota^0(y)$ $(y \in Y)$.

Set

$$F_{\mathcal{C}}(Y) = \varprojlim_{N\in\mathcal{N}} \Phi/N.$$

The compatible family $\Phi \to \Phi/N$ of homomorphisms defines a homomorphism $i\colon \Phi \to F_{\mathcal{C}}(Y)$. Its image is dense in $F_{\mathcal{C}}(Y)$. Take $\iota = i \circ \iota^0$. Clearly ι is convergent to 1. Now we claim that $F_{\mathcal{C}}(Y)$ is free pro-$\mathcal{C}$ on Y: indeed, suppose G is a pro-$\mathcal{C}$ group and let $\varphi\colon Y \to G$ be convergent to 1. Let $\varphi_0\colon \Phi \to G$ be the unique homomorphism such that $\varphi_0 \circ \iota^0 = \varphi$.

$$\begin{tikzcd}
Y \arrow[r, "\iota^0"] \arrow[dr, "\varphi"'] & \Phi \arrow[r, "i"] \arrow[d, "\varphi_0"] & F_{\mathcal{C}}(Y) \arrow[dl, "\bar{\varphi}"] \\
& G &
\end{tikzcd}$$

One checks that $\bar{\varphi}$ is continuous. It is unique because the image of i is dense. $\square$

Lemma 2.10. (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 2.2. 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 2.3, $\bar{\mu}$ 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 2.3.

□

If $F = F_{\mathcal{C}}(X)$ is a free pro-$\mathcal{C}$ group on the set X converging to 1, define the *rank* of F to be the cardinality of X. It is denoted by $\operatorname{rank}(F)$.

Given a cardinal number m, we denote by $F_{\mathcal{C}}(m)$ or $F(m)$ a free pro-$\mathcal{C}$ group (on a set converging to 1) of rank m.

The next result is clear.

Proposition 2.11. *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,* $\operatorname{rank}(\Phi) = \operatorname{rank}(\Phi_{\hat{\mathcal{C}}})$.

Example.

(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.

The following result justifies the apparently artificial definition of free pro-$\mathcal{C}$ group that we have given above: why do we assume that Y converges to 1? [see also the comments at the end of Section 2.5].

Proposition 2.12. *Every pro-$\mathcal{C}$ group G is a quotient of a free pro-$\mathcal{C}$ group.*

This is a consequence of Proposition 2.1.

2.3 The embedding problem

Motivation 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? This is called an *embedding problem.* A slightly different way of posing this question is the following: given the diagram

$$\begin{tikzcd}
 & G_{\bar{F}/F} \arrow[d, two heads, "\varphi"] \\
H' \arrow[r, two heads, "\alpha"] & H = G_{K/F}
\end{tikzcd}$$

is there a continuous epimorphism $\varphi_1 : G_{\bar{F}/F} \to H'$ making the diagram commutative?

This question will be considered by some of my colleagues in this conference. For us it serves as a motivation for the following definitions.

Definition 2.13. Let G be a pro-$\mathcal{C}$ group.

(a) An embedding problem for G is a diagram of pro-$\mathcal{C}$ groups

(2.2)
$$\begin{tikzcd}
 & & & G \arrow[d, two heads, "\varphi"] & \\
1 \arrow[r] & K \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r] & 1
\end{tikzcd}$$

with exact row, where φ is a continuous epimorphism of profinite groups.

(b) We say that the embedding problem (2.2) 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 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 $\alpha\bar{\varphi} = \varphi$.

(c) The kernel of the embedding problem (2.2) is the group $K = \mathrm{Ker}(\alpha)$. We say that the embedding problem (2.2) has 'finite minimal normal kernel' if K is a finite minimal normal subgroup of A.

(d) An infinite pro-$\mathcal{C}$ group G is said to have the 'strong lifting property' if every embedding problem (2.2) with $w_0(B) < w_0(G)$ and $w_0(A) \leq w_0(G)$ is solvable.

Lemma 2.14. *Let G be a pro-$\mathcal{C}$ group. The following conditions are equivalent.*

(a) *G has the strong lifting property;*

(b) *G has the strong lifting property over embedding problems* (2.1) *with finite minimal normal kernel.*

Proof. The implication (a) ⇒ (b) is obvious.

(b) ⇒ (a): Suppose G has the strong lifting property over embedding problems (2.1) with finite minimal normal kernel and let (2.1) be an embedding problem with $w_0(B) < w_0(G)$ and $w_0(A) \leq w_0(G)$. It follows from Theorem 2.5 that there exist an ordinal number μ and a chain of closed subgroups of K (see diagram (2.1))

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

such that

(i) each K_ℓ is a normal subgroup of A with $K_\ell/K_{\ell+1}$ finite; moreover, $K_{\ell+1}$ is maximal in K_ℓ with respect to these properties;

(ii) if ℓ is a limit ordinal, then $K_\ell = \bigcap_{\nu<\ell} K_\nu$; 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 $\ell \leq \mu$ there exists an epimorphism

$$\varphi_\ell : G \longrightarrow A/K_\ell$$

such that if $\ell_1 \leq \ell$ the diagram

$$\begin{tikzcd} & G \arrow[dl, "\varphi_\ell"'] \arrow[dr, "\varphi_{\ell_1}"] & \\ A/K_\ell \arrow[rr] & & A/K_{\ell_1} \end{tikzcd}$$

commutes, where the horizontal mapping is the natural epimorphism. Then we can take $\bar{\varphi} = \varphi_\mu$. To show the existence of φ_ℓ, we proceed by induction (transfinite, if K is infinite) on ℓ. Note that $A/K_0 = B$; so, put $\varphi_0 = \varphi$. Let $\ell \leq \mu$ and assume that φ_ν has been defined for all $\nu < \ell$ so that the above conditions are satisfied. If ℓ is a limit ordinal, observe that since $K_\ell = \bigcap_{\nu<\ell} K_\nu$, then

$$A/K_\ell = \varprojlim_{\nu<\ell} A/K_\nu \ ;$$

in this case, define $\varphi_\ell = \varprojlim_{\nu<\ell} \varphi_\nu$.

If, on the other hand, $\ell = \sigma+1$, we define φ_ℓ to be a solution to the embedding problem with finite minimal normal kernel

$$\begin{tikzcd}
 & & & G \arrow[dl, dotted, "\varphi_\ell"'] \arrow[d, two heads, "\varphi_\sigma"] & \\
1 \arrow[r] & K_\sigma/K_\ell \arrow[r] & A/K_\ell \arrow[r] & A/K_\sigma \arrow[r] & 1
\end{tikzcd}$$

To see that such a solution exists, we have to verify that $w_0(A/K_\sigma) < w_0(G)$ and $w_0(A/K_\ell) \leq w_0(G)$. If $w_0(A) < w_0(G)$, these inequalities are clear. On the other hand, if $w_0(A) = w_0(G)$, we have

$$w_0(A/K_\ell) = w_0(A/K_\sigma) < w_0(A) = w_0(G),$$

since K_σ/K_ℓ is a finite group and since condition (iii) above holds.

It is clear that in either case φ_ℓ satisfies the required conditions. □

2.4 Characterization of free pro-$\mathcal{C}$ groups

Here we present two results that characterize free pro-$\mathcal{C}$ groups on a set converging to 1 in terms of embedding problems.

Theorem 2.15. *(*Finite rank*) Let G be a pro-$\mathcal{C}$ group. Assume that $d(G) = m$ is finite. Then, the following two conditions are equivalent*

(a) *G is a free pro-$\mathcal{C}$ group of rank m;*

(b) *Every embedding problem of pro-$\mathcal{C}$ for G*

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

with $d(B) \leq d(G)$ and $d(A) \leq d(G)$, has a solution.

Proof. (a) ⇒ (b) This implication follows immediately from Proposition 2.4.

(b) ⇒ (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. □

Theorem 2.16 (Mel'nikov). *Let G be a pro-$\mathcal{C}$ group. Assume that $d(G) = m$ is infinite. Then, the following two conditions are equivalent*

(a) *G is a free pro-$\mathcal{C}$ group on a set converging to 1 of rank m;*

(b) *G has the strong lifting property.*

Proof. (a) $\Rightarrow$ (b) Let G be a free pro-$\mathcal{C}$ group of rank m on the set X converging to 1. Then $|X| = w_0(G)$ (see Proposition 2.2). Consider the embedding problem

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

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 2.14 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, $|\mathcal{U}| < m$. Observe that, since X converges to 1,

$$|X - \mathrm{Ker}(\varphi)| = |X - \bigcap_{U\in\mathcal{U}} \varphi^{-1}(U)| = |\bigcup_{U\in\mathcal{U}} (X - \varphi^{-1}(U))| = |\mathcal{U}|.$$

Therefore, $|X_0| = m$. 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 1.14 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 in [5]. □

Combining the theorem above with Lemma 2.14, we get the following characterization of free pro-$\mathcal{C}$ groups of infinite countable rank.

Corollary 2.17 (Iwasawa). *Let $\mathcal{C}$ be a variety 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 pro-$\mathcal{C}$ groups of the form*

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

has a solution whenever A is finite.

2.5 Free pro-$\mathcal{C}$ groups on profinite spaces

Let F be the free pro-$\mathcal{C}$ on the set Y, as described in Definition 2.8, and let $\iota : Y \to F$ be the canonical map. If the class $\mathcal{C}$ contains at least one nontrivial group, it easily follows that ι is injective: indeed, if $x \neq y$ in Y, choose $G \in \mathcal{C}$ and $\varphi : Y \to G$ to be such that $\varphi(x) \neq \varphi(y)$. Then the corresponding homomorphism $\bar{\varphi} : F \to G$ with $\bar{\varphi}\iota = \varphi$, forces $\iota(x) \neq \iota(y)$.

One identifies Y with its image in F, and then the closure $\bar{Y}$ of Y in F is just $X = Y \cup \{1\}$, the one-point compactification of the discrete set Y. These considerations motivate the following apparently more general definition. First some terminology: A pointed topological space $(X, *)$ is a topological space X with a distingished point $* \in X$. A profinite group G can be thought of as a pointed space whose distinguished point is the neutral element 1. A map of pointed spaces is a continuous map that preserves distinguished points.

Definition 2.18. Let $(X, *)$ be a pointed profinite space. A pro-$\mathcal{C}$ group $F = F(X, *)$ together with a map $\iota\colon X \to F$ of pointed spaces is called a *free pro-$\mathcal{C}$ group* on the pointed space $(X, *)$ if it satisfies following universal property: if $\varphi\colon X \to G$ is any continuous map of pointed spaces into a pro-$\mathcal{C}$ group G, then there exists a unique continuous homomorphism $\bar{\varphi}\colon F \to G$ such that the diagram

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

commutes.

We say that $(X, *)$ is a basis for F.

Note that a profinite space X can be thought naturally as a pointed space by adding to it an isolated point: $X \cup \{*\}$. Then we denote the corresponding free pro-$\mathcal{C}$ group $F(X \cup \{*\}, *)$ by $F(X)$, which satisfies an obvious universal property as above, but where the maps are not anymore maps of pointed spaces.

These more general free pro-$\mathcal{C}$ groups are often very useful when trying to describe the subgroup structure of (normal) subgroups of a free pro-$\mathcal{C}$ group (see Chapters 3 and 8 in [5]) . For example, if $F = F(x, y)$ is the free profinite group of rank 2, then the closed normal subgroup of F generated by x can be easily described as a free profinite on a space homeomorphic to $\hat{\mathbf{Z}}$.

However $F = F(X, *)$ can always be described as a free pro-$\mathcal{C}$ on a set in the sense of Definition 2.8, although there is no canonical procedure to find a basis converging to 1 for F. See Proposition 3.5.12 and Theorem 3.5.13 in [5].

2.6 Open subgroups of free pro-$\mathcal{C}$ groups

It is well-known that subgroups of abstract free groups are free. In contrast it is obvious that closed subgroups of a free pro-$\mathcal{C}$ group need not be free pro-$\mathcal{C}$

in general: for example, $\hat{\mathbf{Z}}$ is free profinite, but its p-Sylow subgroup $\mathbf{Z}_p$ is not. However one has the following general result.

First we recall the concept of Schreier transversal. Let $\Phi = \Phi(Y)$ be an abstract free group on a basis Y and let Δ be a subgroup of Φ. Let T be a right transversal of Δ in Φ (i.e., a set of representatives of the right cosets of Δ in Φ). One says that T is a *Schreier transversal* if it closed under taking prefixes (and in particular contains the empty word): if $y_1, \dots, y_n \in Y \cup Y^{-1}$ 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 $i = 0, \dots, n-1$. The existence of Schreier transversals is a standard exercise in Zorn's Lemma.

In the next result we assume that the variety of finite groups $\mathcal{C}$ is 'closed under extensions', i.e., if $1 \to K \to G \to H \to 1$ is an exact sequence of groups and $K, H \in \mathcal{C}$, then $G \in \mathcal{C}$. For example, $\mathcal{C}$ could be the class of all finite groups, or all finite solvable groups, or, for a fixed prime p, all finite p-groups.

Theorem 2.19. *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*

$$B = \{tx(\overline{tx})^{-1} \mid (t, x) \in T \times X\}.$$

Then $1 \in B$, B is a profinite space and H is a free pro-$\mathcal{C}$ on the pointed space $(B, 1)$.

In [5] one can find two different proofs of this theorem. The first one (cf. Section 3.6) depends on the corresponding result for abstract free groups. The second one (cf. Appendix D.2) is better and more elementary: it is based on wreath products and it is done from scratch [in fact this method also gives a proof for the corresponding result in abstract groups: The Nielsen-Schreier theorem].

2.7 Free products of pro-$\mathcal{C}$ groups

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 $\iota_\alpha \colon G_\alpha \longrightarrow G$ 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 $\{\lambda_\alpha \colon G_\alpha \longrightarrow K \mid \alpha \in A\}$ is a convergent family of continuous homomorphisms into a pro-$\mathcal{C}$ group K, then there exists a unique continuous homomorphism $\lambda \colon G \longrightarrow K$ such that

$$\begin{tikzcd}
G_\alpha \arrow[r, "\iota_\alpha"] \arrow[dr, "\lambda_\alpha"'] & G \arrow[d, dotted, "\lambda"] \\
& K
\end{tikzcd}$$

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

$$G^{abs} = \ast_{\alpha \in A} G_\alpha$$

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 $\coprod_{\alpha \in A}^{r} G_\alpha$.

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 $\coprod$.

For such free products, one has the following subgroup theorem

Theorem 2.20. *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.

In [5] one can find two different proofs of this theorem. The first one (cf. [5], Section 9.1) depends on the corresponding result for abstract free groups. The second one (cf. [5], Appendix D.3) is better and more elementary: it is based on wreath products and it is done from scratch [in fact this method also gives a simple proof for the corresponding result in abstract groups: The Kurosh subgroup theorem].

3 Lecture 3

3.1 G-Modules

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

$$\begin{array}{ccc} \text{(i)} & (gh)a & = & g(ha) \\ \text{(ii)} & g(a+b) & = & ga + gb \\ \text{(iii)} & 1a & = & a \end{array}$$

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.

The following lemma is proved easily.

Lemma 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 3.2 (Examples of 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).

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 $\mathbf{DMod}(G)$.

3.2 The complete group algebra

Consider a commutative profinite ring R (for example $R = \hat{\mathbf{Z}}$) 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* 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.

Notation: $\mathbf{DMod}([\![RG]\!])$ is the category of discrete $[\![RG]\!]$-modules and continuous module homomorphisms. $\mathbf{PMod}([\![RG]\!])$ is the category of profinite $[\![RG]\!]$-modules (and continuous module homomorphisms).

Duality Between Discrete and Profinite Modules

Put $\Lambda = [\![RG]\!]$. 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. Then M^* is profinite if M is 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. The contravariant functor $\mathrm{Hom}(-, \mathbf{Q}/\mathbf{Z})$ establishes a "duality" between the categories $\mathbf{PMod}(\Lambda)$ and $\mathbf{DMod}(\Lambda^{op})$. 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.

Proposition 3.3. *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. The most interesting part is (e): Put $\Lambda = [\![RG]\!]$. 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 (e) follows. □

3.3 Projective and injective modules

Let $\mathcal{A}$ be a category. An object P in $\mathcal{A}$ is called *projective* if for every diagram

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

of objects and morphisms in $\mathcal{A}$, 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 $\mathcal{A}$ is an abelian category, one has equivalently, that P is projective in $\mathcal{A}$ 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 $\mathcal{A}$, 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.

One says that a category $\mathcal{A}$ has *enough projectives* if for every object M in $\mathcal{A}$, there exists a projective object P of $\mathcal{A}$ and an epimorphism $P \longrightarrow M$.

Proposition 3.4. *Let* $\Lambda = [\![RG]\!]$.

(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.*

The dual concept of a projective object in a category $\mathcal{A}$ is that of an injective object. An object Q in $\mathcal{A}$ is called *injective* if whenever

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \\ Q & \end{tikzcd}$$

is a diagram of objects and morphisms in $\mathcal{A}$, 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 $\mathcal{A}$ is an abelian category, one has equivalently, that Q is injective in $\mathcal{A}$ 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 $\mathcal{A}$, 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.

One says a category $\mathcal{A}$ has *enough injectives* if for every object M in $\mathcal{A}$, there exists an injective object Q of $\mathcal{A}$ and a monomorphism $M \longrightarrow Q$.

An object M in $\mathbf{DMod}(\Lambda)$ is called *cofree* if it satifies a universal property dual to that of free objets, i.e., if its dual M^* is free in $\mathbf{PMod}(\Lambda)$. Applying duality, Proposition 3.4 yields

Proposition 3.5. *Let* $\Lambda = [\![RG]\!]$.

(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 3.3, $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$ is the subcategory of $\mathbf{DMod}(G)$ consisting of those modules that are torsion.

Proposition 3.6. *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. 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

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r, "\psi"] \arrow[d, "\zeta"] & C \arrow[ddl, dotted, "\xi"] \\
& M_A \arrow[d] & \\
& M &
\end{tikzcd}$$

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 $\xi(C) \subseteq M_A$. □

3.4 Complete tensor product

Let $\Lambda = [\![RG]\!]$. 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 $(a, b) \mapsto a\widehat{\otimes} b$, 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 $\bar{\varphi}(a\widehat{\otimes} b) = \varphi(a, b)$. It is easy to see that if the complete tensor product exists, it is unique up to isomorphism. We denote it by $A\widehat{\otimes}_\Lambda B$. Furthermore, it is clear that $\{a\widehat{\otimes} b \mid a \in A, b \in B\}$ is a set of topological generators for the R-module $A\widehat{\otimes}_\Lambda B$.

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 3.7. *With the above notation, the complete tensor product $A\widehat{\otimes}_\Lambda B$ 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

$$A\widehat{\otimes}_\Lambda B = \varprojlim_{i \in I, j \in J} (A_i \otimes_\Lambda B_j)\ ,$$

where $A_i \otimes_\Lambda B_j$ is the usual tensor product as abstract Λ-modules. In particular, $A\widehat{\otimes}_\Lambda B$ 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*

$$A \otimes_\Lambda B \longrightarrow A_i \otimes_\Lambda B_j \quad (i \in I, j \in J).$$

3.5 Cohomology of profinite groups

Let G be a profinite group and let $A \in \mathbf{DMod}(G)$. For each natural number n we consider an R-module

$$H^n(G, A),$$

the *nth cohomology group of G with coefficients in A.* We shall give explicit definitions of these cohomology groups later in Section 3.6. Here, instead, we mention some of their fundamental properties (cf. Proposition 6.2.2 in [5]), which in fact characterize them:

(a) $H^n(G,A)$ are functors in the variable A;

(b) $H^0(G,A) = \mathrm{Hom}_{[\![RG]\!]}(R,A) = \{a \mid a \in A, ga = a, \forall g \in G\} = A^G \quad$ (G acts on R trivially);

(c) $H^n(G,Q) = 0$ for every discrete injective $[\![RG]\!]$-module Q and $n \geq 1$;

(d) For each short exact sequence $0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0$ in $\mathbf{DMod}(G)$, 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

$$0 \to H^0(G,A_1) \to H^0(G,A_2) \to H^0(G,A_3) \xrightarrow{\delta}$$

$$H^1(G,A_1) \to H^1(G,A_2) \to \cdots$$

is exact; and

(e) For every commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r] \arrow[d, "\alpha"] & A_2 \arrow[r] \arrow[d, "\beta"] & A_3 \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A_1' \arrow[r] & A_2' \arrow[r] & A_3' \arrow[r] & 0
\end{tikzcd}$$

in $\mathbf{DMod}(G)$ with exact rows, the following diagram commutes for every $n \geq 0$

$$\begin{tikzcd}
H^n(G,A_3) \arrow[r, "\delta"] \arrow[d, swap, "H^n(G,\gamma)"] & H^{n+1}(G,A_1) \arrow[d, "H^{n+1}(G,\alpha)"] \\
H^n(G,A_3') \arrow[r, "\delta"] & H^{n+1}(G,A_1')
\end{tikzcd}$$

.

The existence of these cohomology groups follows from the existence of 'enough injectives' in $\mathbf{DMod}(G)$. The sequence $H^0(G,-), H^1(G,-), H^2(G,A), \dots$ is the "sequence of right derived functors of the functor $A \mapsto A^G$ " (cf. [5], Section 6.1).

3.6 Explicit calculation of cohomology groups

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., $x(x_1,\dots,x_n) = (xx_1,\dots,xx_n)$, for $x, x_1, \dots, x_n \in G$). Then L_n is a free profinite $[\![RG]\!]$-module on the profinite space

$$\{(1,x_1,\dots,x_n) \mid x_i \in G\}.$$

Define a sequence $\mathbf{L}(G)$:

$$\cdots \longrightarrow L_n \xrightarrow{\partial_n} L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \xrightarrow{\epsilon} R \longrightarrow 0, \tag{3.1}$$

where

$$\partial_n(x_0, x_1, \dots, x_n) = \sum_{i=0}^{n}(-1)^i(x_0, \dots, \hat{x}_i, \dots, x_n)$$

(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 (3.1) is in fact an exact sequence, a *free $[\![RG]\!]$-resolution of R.*

If one applies the functor $\mathrm{Hom}_{[\![RG]\!]}(-, A) = -^G$ to (3.1), excluding the first term R, one gets the following cochain complex, $\mathbf{C}(G, A)$:

$$0 \longrightarrow C^0(G, A) \longrightarrow \cdots \longrightarrow C^n(G, A) \xrightarrow{\partial^{n+1}} C^{n+1}(G, A) \longrightarrow \cdots \ , \tag{3.2}$$

where $C^n(G, A)$ consists of all continuous maps $f : G^{n+1} \longrightarrow A$ such that

$$f(xx_0, xx_1, \dots, xx_n) = xf(x_0, x_1, \dots, x_n) \quad \text{for all } x, x_i \in G.$$

And

$$(\partial^{n+1} f)(x_0, x_1, \dots, x_{n+1}) = \sum_{i=0}^{n+1}(-1)^i f(x_0, \dots, \hat{x}_i, \dots x_{n+1}) \ .$$

Then one has the following explicit description:

Theorem 3.8. *$H^n(G, A)$ is the n-th cohomology group of the cochain complex* (3.2)*, i.e.,*

$$H^n(G, A) = \mathrm{Ker}(\partial^{n+1})/\mathrm{Im}(\partial^n) \ .$$

(cf. [5], Theorem 6.2.4).

3.7 Homology of profinite groups

The 'dual' of cohomology is homology [we make this precise later]. For a right profinite $[\![RG]\!]$-module B (we write this as $B \in \mathbf{PMod}([\![RG]\!]^{op})$), define

$$B_G = B/\overline{\langle bg - b \mid b \in B, g \in G\rangle}.$$

Then one defines the *n-th homology group $H_n(G, B)$ of G with coefficients in B.* These are in fact R-modules. They have the following basic properties.

$\{H_n(G, -)\}_{n\in\mathbf{N}}$ is the sequence of left derived functors of the functor $B \mapsto B_G$ from $\mathbf{PMod}([\![RG]\!]^{op})$ to $\mathbf{PMod}(R)$. In other words, this sequence is the unique sequence of covariant functors from $\mathbf{PMod}([\![RG]\!]^{op})$ 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

$$\cdots \to H_1(G,B_2) \to H_1(G,B_3) \xrightarrow{\delta} H_0(G,B_1) \to$$

$$H_0(G,B_2) \to H_0(G,B_3) \to 0$$

is exact; and

(d) For every commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & B_1 \arrow[r] \arrow[d, "\alpha"] & B_2 \arrow[r] \arrow[d, "\beta"] & B_3 \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & B_1' \arrow[r] & B_2' \arrow[r] & B_3' \arrow[r] & 0
\end{tikzcd}$$

in $\mathbf{PMod}(\llbracket RG \rrbracket^{op})$ with exact rows, the diagram

$$\begin{tikzcd}
H_{n+1}(G,B_3) \arrow[r, "\delta"] \arrow[d, "H_{n+1}(G,\gamma)"'] & H_n(G,B_1) \arrow[d, "H_n(G,\alpha)"] \\
H_{n+1}(G,B_3') \arrow[r, "\delta"] & H_n(G,B_1')
\end{tikzcd}$$

commutes for every $n \geq 0$.

One can calculate explicitly $H_n(G,B)$ (see for example [5], Theorem 6.3.1) as the n-th homology group of the sequence

$$\cdots \longrightarrow B\widehat{\otimes}_{\llbracket RG \rrbracket} L_{n+1} \longrightarrow B\widehat{\otimes}_{\llbracket RG \rrbracket} L_n \xrightarrow{\partial_n} \cdots \longrightarrow B\widehat{\otimes}_{\llbracket RG \rrbracket} L_0 \longrightarrow 0 \ .$$

Proposition 3.9 (Duality of homology-cohomology). *Let G be a profinite group and let B be a profinite right $\llbracket \widehat{\mathbf{Z}}G \rrbracket$-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.

3.8 Homology and cohomology in low dimensions

$$H^0(G,A)=\{a\in A \mid xa=a, \forall x\in G\}=A^G$$

is the subgroup of elements of A invariant under the action of G.

$$H^1(G,A)=\mathrm{Der}(G,A)/\mathrm{Ider}(G,A)$$

where

$$\mathrm{Der}(G,A)=\{d:G\longrightarrow A \mid d(xy)=xd(y)+d(x), \quad \text{for all} \quad x,y\in G\}$$

(the *group of derivations*), and $\mathrm{Ider}(G,A)$ is the *group of inner derivations* $d_a : G\to A$ defined for each $a\in A$ as $d_a(x)=xa-a$.

Given a finite G-module A, $H^2(G,A)$ is in $1-1$ correspondence with the (equivalence classes of) extensions of A by G, i.e., exact sequences

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

where the action of G on A is precisely the natural action determined by this sequence.

$$H_0(G,B)=B_G$$

$$H_1(G,\widehat{\mathbf{Z}})\cong G/\overline{[G,G]},$$

the abelianized group of G (here the action of G on $\widehat{\mathbf{Z}}$ is assumed to be trivial)

If G is a pro-p group and the action of G on $\mathbf{F}_p$ is trivial, one has

$$H_1(G,\mathbf{F}_p)\cong G/G^p\overline{[G,G]}.$$

Note that $G^p\overline{[G,G]}=\Phi(G)$ is the Frattini subgroup of G.

For proofs of the above results see [5], Section 6.8.

3.9 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

$$\mathrm{Coind}_H^G(A) =$$

$$\{f : G \longrightarrow A \mid f \text{ continuous, with } f(hy) = hf(y) \text{ for all } h \in H,\ y \in G\}.$$

The compact-open topology makes $\mathrm{Coind}_H^G(A)$ into a discrete abelian group. Define an action of G on $\mathrm{Coind}_H^G(A)$ by

$$(xf)(y) = f(yx) \quad (x, y \in G,\ f \in \mathrm{Coind}_H^G(A)).$$

This action is in fact continuous. So $\mathrm{Coind}_H^G(-)$ transforms modules in $\mathbf{DMod}(H)$ into modules in $\mathbf{DMod}(G)$. The G-module $\mathrm{Coind}_H^G(A)$ is called a *coinduced* module. Its most important property is

Theorem 3.10 (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*

$$H^n(G, \mathrm{Coind}_H^G(A)) \cong H^n(H, A) \quad (n \geq 0).$$

Corollary 3.11. *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 $n > 0$.*

Because of this last property, the coinduced modules of the form $C(G, A)$ play an important role that allows a 'shift of dimension' (using the properties in Section 3.5).

Dually one has *induced modules*: Let $H \leq G$ 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

$$\mathrm{Ind}_H^G(B) = B \widehat{\otimes}_{[\![\widehat{\mathbf{Z}}H]\!]} [\![\widehat{\mathbf{Z}}G]\!].$$

Theorem 3.12. *Let G be a profinite group, H a closed subgroup of G and $B \in \mathbf{PMod}([\![\widehat{\mathbf{Z}}H]\!])$.*

(a) (Shapiro's Lemma) *There exist natural isomorphisms*

$$H_n(G, \mathrm{Ind}_H^G(B)) \cong H_n(H, B), \quad (n \geq 0).$$

(b) *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 $n > 0$.

(cf. [5], Section 6.10).

3.10 Cohomological dimension

Let G be a profinite group and let p be a prime number. If X is an abelian group, we denote by X_p its p-primary part, i.e., the subgroup of X consisting of its elements whose order is a power of p. 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

$$scd(G) = \sup_p scd_p(G).$$

Proposition 3.13. *Let G be a profinite group and let p be a prime. Then*

$$cd_p(G) \le scd_p(G) \le cd_p(G) + 1.$$

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 the multiplication by p. Denote the kernel of this map $A[p]$; in other words,

$$A[p] = \{a \in A \mid pa = 0\}.$$

Consider the short exact sequences

$$0 \longrightarrow A[p] \longrightarrow A \xrightarrow{p} pA \longrightarrow 0,$$

$$0 \longrightarrow pA \longrightarrow A \longrightarrow A/pA \longrightarrow 0.$$

Then $A[p]$ and A/pA are in $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$, in fact they are annihilated by p. So, if $k \ge n$,

$$H^k(G, A[p]) = H^k(G, A/pA) = 0.$$

Therefore, from the long exact sequences corresponding to the short exact sequences above,

$$\cdots \longrightarrow H^k(G, A[p]) \longrightarrow H^k(G,A) \xrightarrow{\varphi} H^k(G,pA) \longrightarrow \cdots$$

$$\cdots \longrightarrow H^{k-1}(G, A/pA) \longrightarrow H^k(G,pA) \xrightarrow{\psi} H^k(G,A) \longrightarrow \cdots,$$

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 the multiplication by p. Thus

$$H^k(G,A)_p = 0, \quad \text{if } k > n.$$

Hence the second inequality follows. □

Example. Let $G = \widehat{\mathbf{Z}}$. Then it is not hard to see that $cd_p(G) = 1$, while $scd_p(G) = 2$ (see [5], Example 7.1.3).

3.11 Cohomological dimension and subgroups

Let H be a closed subgroup of a profinite group G. Then every G-module A is automatically an H-module. From the explicit definition of $H^n(G,A)$ in terms of cochains (see Section 3.6 above) one sees that there are natural homomorphisms (called 'restrictions')

$$\mathrm{Res} \;=\; \mathrm{Res}^G_H : H^n(G,A) \longrightarrow H^n(H,A) \quad (n \geq 0).$$

On the other hand, if H is an open subgroup of a profinite group G, and $A \in \mathbf{DMod}(G)$, then there are natural homomorphisms (called 'corestrictions')

$$\mathrm{Cor} = \;\mathrm{Cor}^H_G : \mathbf{H}^n(H,A) \longrightarrow \mathbf{H}^n(G,A) \quad (n \geq 0).$$

At level 0, corestriction is just the map:

$$\mathrm{N}_{G/H} : A^H \longrightarrow A^G$$

given by

$$\mathrm{N}_{G/H}(a) = \sum ta,$$

where $a \in A^H$ and t runs through a left transversal of H in G.

The fundamental connection between restriction and corestriction is (see [5], Theorem 6.7.3)

Theorem 3.14. *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.,*

$$\mathrm{Cor}^H_G \mathrm{Res}^G_H = [G : H] \cdot \mathrm{id},$$

where id *is the identity on $H^n(G,-)$ $(n \geq 0)$.*

From this one obtains (see [5], Theorem 7.3.1 and Corollary 7.3.3)

Theorem 3.15. *Let G be a profinite group, H a closed subgroup of G and p a prime number. Then*

(a)

$$cd_p(H) \leq \ cd_p(G).$$

Moreover, equality holds in either of the following cases

(1) $p \not| \, [G : H]$,

(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).

(b) *Let* G_p *be a* p*-Sylow group of* G*. Then*

$$cd_p(G) = cd_p(G_p) = cd(G_p).$$

3.12 Projective profinite groups

A pro-$\mathcal{C}$ group G is called $\mathcal{C}$*-projective* if it is a projective object in the category of pro-$\mathcal{C}$ groups, i.e., if every diagram

(3.3)

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

of pro-$\mathcal{C}$ groups has a weak solution. We say that G is *projective* if it is projective in the category of profinite groups (i.e., $\mathcal{C}$-projective and $\mathcal{C}$ is the class of all finite groups).

The following lemma simplifies the criteria to decide whether G is projective.

Lemma 3.16. *Let* $\mathcal{C}$ *and* $\mathcal{C}'$ *be varieties of finite groups, and let* G *be a profinite group. The following conditions are equivalent.*

(a) *Every embedding problem* (3.3) *for* G *where* K *is pro-*$\mathcal{C}'$ *and* A *is pro-*$\mathcal{C}$ *has a weak solution;*

(b) *Every embedding problem* (3.3) *for* G *such that* $A \in \mathcal{C}$ *and* $K \in \mathcal{C}'$ *is an abelian minimal normal subgroup of* A*, has a weak solution.*

Example. A free pro-$\mathcal{C}$ group is $\mathcal{C}$-projective.

Lemma 3.17. *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. 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 Proposition 2.12, 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 $G \leq_c F$, where F is a free pro-$\mathcal{C}$ group. Consider an embedding problem (3.3) as above with $A \in \mathcal{C}$. Then $\mathrm{Ker}(\varphi)$ is an open normal subgroup of G. Hence there exists $V \lhd_o F$ such that $V \cap G \leq \mathrm{Ker}(\varphi)$. 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 2.19). Therefore we may assume that $F = GV$. Put $U = V\mathrm{Ker}(\varphi)$. Then $U \lhd_o F$ 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 (3.3), as needed. □

For certain varieties $\mathcal{C}$ (the so called 'saturated' varieties of finite groups: G finite and $G/\Phi(G) \in \mathcal{C} \Rightarrow G \in \mathcal{C}$), e.g., extension-closed varieties, the distinction between 'projective' and '$\mathcal{C}$-projective' is non-existent. In fact we have (see [5], Proposition 7.6.7).

Proposition 3.18. *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) *$cd(G) \leq 1$.*

Theorem 3.19 (cf. [5], Theorem 7.7.4)**.** *Let G be a pro-p group. Then, the following statements are equivalent*

(a) $\mathrm{cd}_p(G) \leq 1$*;*

(b) $H^2(G, \mathbf{F}_p) = 0$*;*

(c) *G is a free pro-p group;*

(d) *G is a projective group.*

Corollary 3.20 (cf. [5], Corollary 7.7.5)**.** *Every closed subgroup H of a free pro-p group G is a free pro-p group.*

4 References

[1] M.D. Fried and M. Jarden, *Field Arithmetic*, 3rd. ed., Springer, Berlin, 2008.

[2] H. Koch, *Galois theory of p-extensions*, Springer, Berlin, 2002.

[3] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Springer, Berlin, 2008.

[4] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology*, 2nd ed., Queen's Papers in Pure and Appl. Math., Kingston, 1999.

[5] L. Ribes and P. Zalesskii, *Profinite Groups*, 2nd ed., Springer, Berlin, 2010.

[6] J-P. Serre, *Cohomology Galoisienne*, 5th. ed., Springer, Berlin, 1994.

[7] S.S. Shatz, *Profinite Groups, Arithmetic and Geometry*, Princeton Univ. Press, Princeton, 1972.

[8] J.S. Wilson, *Profinite Groups*, Clarendon Press, Oxford 1998.

Luis Ribes
School of Mathematics and Statistics, Carleton University,
Ottawa ON K1V 8N2 Canada
lribes@math.carleton.ca