Winter School on Galois Theory
Luxembourg, 15 - 24 February 2012

INTRODUCTION TO PROFINITE GROUPS

Luis Ribes
Carleton University, Ottawa, Canada

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, but it is not procyclic.

Remark that 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.

2.1.1 Proposition *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 $N \lhd_c G$ 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 $K \leq U \lhd_o G$; 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 $U \lhd_o G$ 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.

2.1.2 Proposition *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 [RZ].

2.1.3 Proposition (**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, say n, in G. Therefore $U = \varphi^{-1}(V)$ for some open normal subgroup V, and thus $U \geq \mathrm{Ker}(\varphi)$, as desired. Hence φ is an injection. Thus φ is a bijection. Since G is compact, it follows that φ is a homeomorphism, and so an isomorphism of profinite groups. □

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

Proof.

Case 1. G is finite.

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

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

such that $\langle g_1, \ldots, g_n \rangle = G$ and $\varphi(g_i) = h_i$ for all i. Let $\mathbf{g} = (g_1, \ldots, g_n) \in G \times \cdots \times G$ be a tuple such that $\varphi(g_i) = h_i$ for all i; then any tuple $\mathbf{g}' = (g_1', \ldots, g_n')$ with $\varphi(g_i') = h_i$ $(i = 1, \ldots, n)$ 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 $\mathbf{g} = (g_1, \ldots, g_n)$ and $g_1, \ldots, g_n$ 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 $H/\varphi(U) = \langle h_1^U, \ldots, h_n^U \rangle$. Let $\mathcal{X}_U$ be the set of all n-tuples $(y_1, \ldots, y_n) \in G/U \times \cdots \times G/U$ such that $\langle y_1, \ldots, y_n \rangle = G/U$ and $\varphi(y_i) = h_i^U$ $(i = 1, \ldots, n)$.

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 1.6.2 that there exists some

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

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

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 [RZ], Theorem 2.6.4 and Corollary 2.6.6.

2.1.5 Theorem *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 $\lambda \leq \mu$*

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

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

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

2.1.6 Corollary *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.

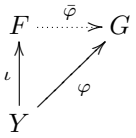
2.2 FREE PRO-$\mathcal{C}$ GROUPS

2.2.1 Definition

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

2.2.2 Definition

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



commutes.

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

Proof. (Sketch) If $\iota: A \to F$ and $\iota': A \to F'$ are free pro-$\mathcal{C}$ groups on Y, let $\psi: F \to F'$ and $\psi': F' \to F$ 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 $\iota^0: Y \to \Phi$ be the abstract free group with basis Y and denote by $\mathcal{N}$ the system of all normal subgroups N of F such that

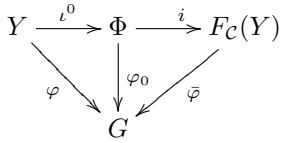
(1) $\Phi/N \in \mathcal{C}$, and

(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 $i: \Phi \to F_{\mathcal{C}}(Y)$. 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 $\varphi: Y \to G$ be convergent to 1. Let $\varphi_0: \Phi \to G$ be the unique homomorphism such that $\varphi_0 \circ \iota^0 = \varphi$.



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

2.2.4 Lemma

(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 $X = \{x_1, \ldots, x_n\}$. Then, any set of generators $\{y_1, \ldots, y_n\}$ 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 2.1.2. Say that $X = \{x_1, \ldots, x_n\}$ is finite and assume that $|Y| > n$. We show that this is not possible. Indeed, choose a subset $X' = \{x'_1, \ldots, x'_n\}$ of Y, and define a map $\mu : Y \longrightarrow F$ by $\mu(x'_i) = x_i$ $(i = 1, \ldots, n)$ 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 2.1.3, $\bar{\mu}$ is an isomorphism, a contradiction.

(b) Consider the continuous epimorphism $\psi : F \longrightarrow F$ determined by $\psi(x_i) = y_i$ $(i = 1, \ldots, n)$. Then ψ is an isomorphism by Proposition 2.1.3. □

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 $\mathrm{rank}(F)$.

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.

2.2.5 Proposition *Let Φ be an abstract free group on a finite basis X. Then the pro-$\mathcal{C}$ completion $\Phi_{\hat{\mathcal{C}}}$ of Φ is a free pro-$\mathcal{C}$ group on X. In particular,* $\mathrm{rank}(\Phi) = \mathrm{rank}(\Phi_{\hat{\mathcal{C}}})$.

Examples

(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].

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

This is a consequence of Proposition 2.1.1.

2.3 THE EMBEDDING PROBLEM

2.3.1 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

$$\begin{array}{ccc} & & G_{\bar{F}/F} \\ & & \big\downarrow \varphi \\ H' & \xrightarrow{\alpha} & H = G_{K/F} \end{array}$$

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.

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

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

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \big\downarrow \varphi & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array} \tag{2}$$

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

(b) *We say that the embedding problem* (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) *is the group $K = \mathrm{Ker}(\alpha)$. We say that the embedding problem* (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) *with $w_0(B) < w_0(G)$ and $w_0(A) \leq w_0(G)$ is solvable.*

2.3.3 Lemma *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* (1) *with finite minimal normal kernel.*

Proof. The implication (a) $\Rightarrow$ (b) is obvious.

(b) $\Rightarrow$ (a): Suppose G has the strong lifting property over embedding problems (1) with finite minimal normal kernel and let (1) be an embedding problem with $w_0(B) < w_0(G)$ and $w_0(A) \leq w_0(G)$. It follows from Theorem 2.1.5 that there exist an ordinal number μ and a chain of closed subgroups of K (see diagram (1))

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

such that

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

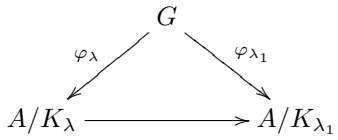
(ii) if λ is a limit ordinal, then $K_\lambda = \bigcap_{\nu<\lambda} K_\nu$; and

(iii) if $w_0(A) = w_0(G)$ (therefore K is an infinite group and $w_0(A/K) < w_0(A)$), then $w_0(A/K_\lambda) < w_0(A)$ whenever $\lambda < \mu$.

We must prove that there exists an epimorphism $\bar{\varphi} : G \longrightarrow A$ such that $\alpha\bar{\varphi} = \varphi$. To do this we show in fact that for each $\lambda \leq \mu$ there exists an epimorphism

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

such that if $\lambda_1 \leq \lambda$ the diagram

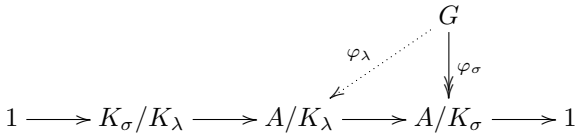


commutes, where the horizontal mapping is the natural epimorphism. Then we can take $\bar{\varphi} = \varphi_\mu$. To show the existence of φ_λ, we proceed by induction (transfinite, if K is infinite) on λ. Note that $A/K_0 = B$; so, put $\varphi_0 = \varphi$. Let $\lambda \leq \mu$ and assume that φ_ν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

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

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

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



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

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

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

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

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.

2.4.1 Theorem (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*

$$\begin{array}{ccccccccc} & & & & & & & & G \\ & & & & & & & & \downarrow \varphi \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array}$$

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

Proof.

(a) $\Rightarrow$ (b) This implication follows immediately from Proposition 2.1.4.

(b) $\Rightarrow$ (a) Consider a free pro-$\mathcal{C}$ group F of rank m, and let $\alpha : F \longrightarrow G$ be a continuous epimorphism. By (b) there exists an continuous epimorphism $\varphi : G \longrightarrow F$ such that $\alpha\varphi = \mathrm{id}_G$. Then φ is a monomorphism, and thus an isomorphism. □

2.4.2 Theorem (**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 2.1.2). Consider the mbedding problem

$$\begin{array}{ccccccccc} & & & & & & & & G \\ & & & & & & & & \downarrow \varphi \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array}$$

with $w_0(B) < w_0(G)$ and $w_0(A) \leq w_0(G)$. We must show that there exists a continuous epimorphism $\bar{\varphi} : G \longrightarrow A$ such that $\alpha\bar{\varphi} = \varphi$. According to Lemma 2.3.3 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, $|\mathcal{U}| < \Updownarrow$. 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 1.4.2 there exists a continuous section $\sigma : B \longrightarrow A$ of α. Think of K as a subgroup of A. Define $\varphi_1 : X \longrightarrow A$ as a map that sends Y to Z bijectively, and such that $\varphi_1 = \sigma\varphi$ on $X - Y$. Since X is a set converging to 1 and φ and σ are continuous, the mapping φ_1 converges to 1. Therefore, φ_1 extends to a continuous homomorphism $\bar{\varphi} : G \longrightarrow A$ with $\alpha\bar{\varphi} = \varphi$. Finally note that $\bar{\varphi}$ is onto since $\varphi_1(X)$ generates A.

(b) $\Rightarrow$ (a) This follows immediately from Corollary 3.5.7 in [RZ]. □

Combining the theorem above with Lemma 2.3.3, we get the following characterization of free pro-$\mathcal{C}$ groups of infinite countable rank.

2.4.3 Corollary (**Iwasawa**) *Let $\mathcal{C}$ be a formation of finite groups and let G be a pro-$\mathcal{C}$ group with $w_0(G) = \aleph_0$. Then G is a free pro-$\mathcal{C}$ group on a countably infinite set converging to 1 if and only if every embedding problem of pro-$\mathcal{C}$ groups of the form*

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array}$$

has a solution whenever A is finite.

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 2.2.2, 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: 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 distinguished 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.

2.5.1 Definition

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

$$\begin{array}{ccc} F & \overset{\bar{\varphi}}{\dashrightarrow} & G \\ {\scriptstyle \iota}\uparrow & \nearrow{\scriptstyle \varphi} & \\ X & & \end{array}$$

commutes.

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

Note that 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 [RZ]) . 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 2.2.2, 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 [RZ].

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 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 $y_1, \ldots, y_n \in Y \cup Y^{-1}$ and $y_1 \cdots y_i \cdots y_n \in T$ is a word in reduced form, then $y_1 \cdots y_i \in T$, for all $i = 0, \ldots, n-1$. The existence of Schreier transversals is a standard exercise in Zorn's Lemma.

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.

2.6.1 Theorem *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*

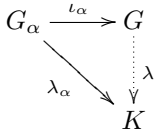
$$B = \{tx(\overline{tx})^{-1} \mid (t, x) \in T \times X\}.$$

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

In [RZ] 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 $\iota_\alpha : G_\alpha \longrightarrow G$ be a continuous homomorphism. One says that the family $\{\iota_\alpha \mid \alpha \in A\}$ is *convergent* if whenever U is an open neighborhood of 1 in G, then U contains all but a finite number of the images $\iota_\alpha(G_\alpha)$. We say that G together with the ι_α is the *free pro-$\mathcal{C}$ product* of the groups G_α if the following universal property is satisfied: whenever $\{\lambda_\alpha : G_\alpha \longrightarrow K \mid \alpha \in A\}$ is a convergent family of continuous homomorphisms into a pro-$\mathcal{C}$ group K, then there exists a unique continuous homomorphism $\lambda : G \longrightarrow K$ such that



commutes, for all $\alpha \in A$. One easily sees that if such a free product exists, then the maps ι_α are injections. We denote such a free pro-$\mathcal{C}$ product again by

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

Free pro-$\mathcal{C}$ products exist and are unique. To construct the free pro-$\mathcal{C}$ product G one proceeds as follows: let

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

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 $\coprod^r_{\alpha\in A} G_\alpha$.

If the set A is finite, the 'convergence' property of the homomorphisms ι_α is automatic; in that case, instead of $\coprod^r$, we use the symbol $\coprod$.

For such free products, one has the following subgroup theorem

2.7.1 Theorem *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

$$H = \left[\coprod^r_{\alpha\in A, u\in D_\alpha} uG_\alpha u^{-1} \cap H\right] \amalg F,$$

where F is a free pro-$\mathcal{C}$ group of finite rank.

In [RZ] one can find two different proofs of this theorem. The first one (cf. Section 9.1) depends on the corresponding result for abstract free groups. The second one (cf. 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].