2 Profinite Groups

2.1 Pro-$\mathcal{C}$ Groups

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

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

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

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

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

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

($\mathcal{C}1$) $\mathcal{C}$ is subgroup closed.

($\mathcal{C}2$) $\mathcal{C}$ is closed under taking quotients, that is, if $G \in \mathcal{C}$ and $K \lhd G$, then $G/K \in \mathcal{C}$.

($\mathcal{C}3$) $\mathcal{C}$ is closed under forming finite direct products, that is, if $G_i \in \mathcal{C}$ ($i = 1, \ldots, n$), then

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lemma 2.1.1 *Let*

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

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

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

be the projection homomorphisms. Then

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

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

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

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

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

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

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

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

□

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

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

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

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

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

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

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

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

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

Proof. (a) ⇒ (b): Say

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

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

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

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

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

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

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

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

$$VW^n \subseteq V,$$

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

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

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

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

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

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

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

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

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

are compatible, they induce a continuous homomorphism

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$H \leq_o G, \qquad H \leq_c G, \qquad H \lhd_o G, \qquad H \lhd_c G, \qquad H \leq_f G, \qquad H \lhd_f G,$$

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

Proposition 2.1.5

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

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

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

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

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

Example 2.1.6 (Completions)

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

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

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

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

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

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

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

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

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

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

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

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

is a pro-p group.

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

Exercise 2.1.8

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

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

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

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

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

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

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

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

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

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

Exercise 2.1.9

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

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

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

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

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

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

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

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

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

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

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

(d) *The inverse limit*

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

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

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

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

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

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

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

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

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

(e) Let

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

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

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

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

Existence of Sections

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

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

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

be the canonical projection. Then π admits a continuous section

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

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

Proof. We divide the proof into two parts. Assume first that H is a finite group. Then there exists an open normal subgroup U of G such that $U \cap H = 1$. Therefore the restriction $\pi|_U$ is injective. Since U is compact, the

restriction $\pi|_U : U \longrightarrow \pi(U)$ is an isomorphism of topological groups. Hence, there is a continuous inverse isomorphism $\sigma : \pi(U) \longrightarrow U$ of $\pi|_U$. Since $\pi(U)$ is an open (normal) subgroup of G/H, one can express G/H as a finite disjoint union of the left cosets of $\pi(U)$. Consequently, σ admits a continuous extension, by translation, to the whole of G/H. This extension is a section of π, which we denote still by σ. Clearly, $\sigma(1H) = 1$.

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

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

and the diagram

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

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

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

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

$$G/K = \varprojlim_I G/K_i.$$

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

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

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

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

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

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

to the projection

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

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

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

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

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

Exactness of Inverse Limits of Profinite Groups

Let

$$1 \longrightarrow \{G_i, \varphi_{ij}, I\} \xrightarrow{\Theta} \{G'_i, \varphi'_{ij}, I\} \xrightarrow{\Psi} \{G''_i, \varphi''_{ij}, I\} \longrightarrow 1 \tag{1}$$

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

$$1 \longrightarrow G_i \xrightarrow{\theta_i} G'_i \xrightarrow{\psi_i} G''_i \longrightarrow 1$$

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

$$1 \longrightarrow \varprojlim_{i \in I} G_i \xrightarrow{\theta} \varprojlim_{i \in I} G'_i \xrightarrow{\psi} \varprojlim_{i \in I} G''_i \longrightarrow 1, \tag{2}$$

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

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

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

2.3 The Order of a Profinite Group and Sylow Subgroups

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

Proposition 2.3.1 *Let G be a profinite group.*

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

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

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

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

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

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

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

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

On the other hand,

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

a contradiction. □

Consider a profinite group

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

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

A *supernatural number* is a formal product

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

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

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

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

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

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

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

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

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

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

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

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

Proposition 2.3.2 *Let G be a profinite group.*

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

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

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

(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. 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,*

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

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

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

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

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

Hence, it suffices to prove that

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

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

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

and

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

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

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

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

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

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

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

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

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

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

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

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

(a) *Suppose that*

$$G = \varprojlim_I G_i,$$

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

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

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

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

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

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

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

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

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

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

Then

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The methods used in Theorem 2.3.5 give an indication of how certain properties valid for the finite groups in a class $\mathcal{C}$, can be generalized to pro-$\mathcal{C}$ groups. The general philosophy is that, if a property is shared by the groups of an inverse system $\{G_i, \varphi_{ij}\}$ of groups, and this property is preserved by the homomorphisms φ_{ij} in some "uniform" manner, then that property will imply a judiciously phrased analogous one for the corresponding inverse

limit $\varprojlim G_i$. As further applications of these methods, we mention a few more results that it will be convenient to have explicitly stated for future reference. In most cases we leave the proofs as exercises, although we shall remind the reader of the necessary corresponding properties of finite groups.

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

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

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

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

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

(a) *For each prime q,*

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

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

$$S_2 S_3 S_5 \cdots$$

of all the groups S_q is G.

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

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

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

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

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

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

Note that

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

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

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

Exercise 2.3.12

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

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

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

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

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

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

(c) $|\mathrm{GL}_n(\mathbf{Z}/p^m\mathbf{Z})| = p^{(m-1)n^2}(p^n - 1)(p^n - p)\cdots(p^n - p^{n-1})$;
(d) The profinite group $\mathrm{GL}_n(\mathbf{Z}_p)$ has a p-Sylow subgroup of index

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

(Hint: see Exercise 2.1.9.)

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

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

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

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

(a) Let p be a prime number and assume that S is a p-Sylow subgroup of G. Let $\varphi : G \longrightarrow H$ be a continuous epimorphism of profinite groups. Prove that if W is weakly c (respectively, strongly c) in S with respect to G, then $\varphi(W)$ is weakly c (respectively, strongly c) in $\varphi(S)$ with respect to H.

(b) The properties of being weak and strong c are preserved by inverse limits. Explicitly: assume that

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) G is pronilpotent;
(b)

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

2.4 Generators

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

Lemma 2.4.1

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

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

Denote by $\varphi_i : G \longrightarrow G_i$ $(i \in I)$ *the projection maps. Let* $X \subseteq G$. *Then* X *generates* G *if and only if* $\varphi_i(X)$ *generates* G_i *for each* $i \in I$.
(b) *Let* X *be a subset of a profinite group* G *and let* $\bar{X}$ *denote its closure. Then* X *generates* G *if and only if* $\bar{X}$ *generates* G.

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

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

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

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

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

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

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

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

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

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

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

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

2.5 Finitely Generated Profinite Groups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\varphi : G \longrightarrow H$$

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

Proof.

Case 1. G is finite.

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

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

such that $\langle g_1, \ldots, g_n \rangle = G$ 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 1.1.4 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 $G = \overline{\langle g_1, \ldots, g_n \rangle}$. □

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

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

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

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

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

2.6 Generators and Chains of Subgroups

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

Proposition 2.6.1

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

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

(b) Let $\mathcal{N}$ be a fundamental system of neighborhoods of 1 consisting of open normal subgroups. Then $\{gN \mid N \in \mathcal{N}\}$ is a base of open sets of G. The cardinality of this base is still $w_0(G)$ since each $N \in \mathcal{N}$ has finite index

in G. So $w_0(G) \geq w(G)$, and therefore $w_0(G) = w(G)$. By part (a), the result follows. □

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

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

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

$$\varphi : G \longrightarrow H$$

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

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

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

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

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

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

such that

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

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

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

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

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

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

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

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

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

since λ is infinite. □

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

Corollary 2.6.5 *Let $\mathcal{C}$ be a formation of finite groups closed under taking normal subgroups. Assume that G is a pro-$\mathcal{C}$ group and let H be a closed*

normal subgroup of G. Then there exists an ordinal number μ and a chain of closed pro-$\mathcal{C}$ subgroups H_λ of H

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

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

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

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

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

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

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

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

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

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

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

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

is a fundamental system of open neighborhoods of 1 in H. Hence $w_0(G) \geq w_0(H) + w_0(G/H)$. Thus $w_0(G) = w_0(H) + w_0(G/H)$. Part (e) is proved as in

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

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

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

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

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

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

2.7 Procyclic Groups

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

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

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

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

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

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

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

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

Statement (c) follows from (b).

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

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

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

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

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

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

2.8 The Frattini Subgroup of a Profinite Group

Let G be a profinite group. According to Proposition 2.1.4, every closed subgroup of G is the intersection of open subgroups; hence a maximal closed subgroup of G is necessarily open. Moreover, if G is nontrivial, it always has

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

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

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

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

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

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

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

Proposition 2.8.2

(a) *Let G be a profinite group. If $N \lhd_c G$ and $N \leq \Phi(G)$, then $\Phi(G/N) = \Phi(G)/N$.*

(b) *If $\rho : G \longrightarrow H$ is an epimorphism of profinite groups, then $\rho(\Phi(G)) \leq \Phi(H)$.*

(c) *If $\{G_i, \varphi_{ij}, I\}$ is a surjective inverse system of profinite groups over the directed indexing set I, then*

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

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

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

$$\varphi_i : G \longrightarrow G_i$$

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

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

Consider now an element

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

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

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

□

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

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

where U runs through the open normal subgroups of G.

Proof. Consider the short exact sequence

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

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

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

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

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

Proof. Express G as

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

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

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

□

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

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

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

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

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

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

(b)

$$G/\Phi(G) = G/\bigcap M \hookrightarrow \prod G/M,$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Then

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

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

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

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

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

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

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

2.9 Pontryagin Duality for Profinite Groups

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

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

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

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

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

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

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

Given a group G, define a mapping

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

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

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

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

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

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

Proposition 2.9.1

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

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

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

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

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

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

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

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

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

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

Lemma 2.9.3

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

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

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

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

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

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

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

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

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

be a homomorphism. Denote by f_j the composition

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

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

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

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

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

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

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

Lemma 2.9.4

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

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

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

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

Example 2.9.5

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

Theorem 2.9.6 (Pontryagin Duality for Profinite Groups)

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

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

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

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

is an isomorphism.

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

Consider now a profinite abelian group G and express it as

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

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

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

Using Lemma 2.9.3, one deduces that

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

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

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

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

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

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

So, using again Lemma 2.9.3,

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

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

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

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

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

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

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

As an immediate consequence of the lemma above we have

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

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

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

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

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

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

where the penultimate equality follows from Corollary 2.9.8. □

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

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

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

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

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

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

as needed. □

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

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

and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

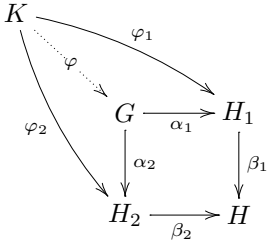
2.10 Pullbacks and Pushouts

In this section we establish the concepts of pullback and pushout diagrams. We do this only for profinite groups and we leave to the reader the development of the analogous constructions for other categories, like modules, graphs, etc. For a more general treatment of these concepts in a category, see for example Mac Lane [1971].

A commutative square diagram

$$\begin{array}{ccc} G & \xrightarrow{\alpha_1} & H_1 \\ {\scriptstyle\alpha_2}\downarrow & & \downarrow{\scriptstyle\beta_1} \\ H_2 & \xrightarrow[\beta_2]{} & H \end{array} \tag{4}$$

of profinite groups and continuous homomorphisms is called a *pullback diagram* or a *pullback of* β_1 *and* β_2 if the following universal property is satisfied:



whenever K is a profinite group and $\varphi_i : K \longrightarrow H_i$ $(i = 1, 2)$ are continuous homomorphisms such that $\beta_1\varphi_1 = \beta_2\varphi_2$, then there exists a unique continuous homomorphism $\varphi : K \longrightarrow G$ such that $\alpha_1\varphi = \varphi_1$ and $\alpha_2\varphi = \varphi_2$.

We say that φ is the canonical homomorphism determined by φ_1 and φ_2. Given two continuous homomorphisms of profinite groups $\beta_i : H_i \longrightarrow H$, there exists a (essentially unique) pullback of β_1 and β_2. Indeed, define

$$P = \{(h_1, h_2) \in H_1 \times H_2 \mid \beta_1(h_1) = \beta_2(h_2)\};$$

and let $\gamma_i : P \longrightarrow H_i$ be given by $\gamma_i(h_1, h_2) = h_i$ $(i = 1, 2)$. Then

$$\begin{array}{ccc} P & \xrightarrow{\gamma_1} & H_1 \\ {\scriptstyle\gamma_2}\downarrow & & \downarrow{\scriptstyle\beta_1} \\ H_2 & \xrightarrow[\beta_2]{} & H \end{array}$$

is a pullback diagram, as one easily checks. It is unique in the sense that if (4) is also a pullback of β_1 and β_2, then there exists a continuous homomorphism

$$\alpha : G \longrightarrow P$$

such that $\gamma_i\alpha = \alpha_i$ $(i = 1, 2)$; namely α is given $\alpha(g) = (\alpha_1(g), \alpha_2(g))$; moreover, one verifies with no difficulty that α is an isomorphism.

Exercise 2.10.1 Let U, V be closed normal subgroups of a profinite group G. Then the commutative square of natural epimorphisms

$$\begin{array}{ccc} G/U \cap V & \longrightarrow & G/U \\ \downarrow & & \downarrow \\ G/V & \longrightarrow & G/UV \end{array}$$

is a pullback diagram.

Lemma 2.10.2 *Assume that* (4) *is a pullback diagram of profinite groups. Let A be a profinite group and let $\varphi_i : A \longrightarrow H_i$ $(i = 1, 2)$ be continuous epimorphisms such that $\beta_1\varphi_1 = \beta_2\varphi_2$ and $\mathrm{Ker}(\beta_1\varphi_1) = \mathrm{Ker}(\varphi_1)\mathrm{Ker}(\varphi_2)$. Then the canonical homomorphism $\varphi : A \longrightarrow G$ determined by φ_1 and φ_2 is an epimorphism.*

Proof. As pointed out above, G can be identified with

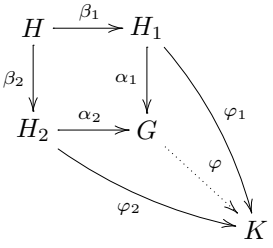
$$\{(h_1, h_2) \in H_1 \times H_2 \mid \beta_1(h_1) = \beta_2(h_2)\}$$

and α_1 and α_2 with the natural projections. Note that in this case, $\varphi(a) = (\varphi_1(a), \varphi_2(a))$, for all $a \in A$. Since $\alpha_1\varphi = \varphi_1$ is onto, to prove that φ is an epimorphism, it suffices to show that $\mathrm{Ker}(\alpha_1) \leq \varphi(A)$; in fact we shall show that $\mathrm{Ker}(\beta_1\alpha_1) \leq \varphi(A)$. Let $(h_1, h_2) \in \mathrm{Ker}(\beta_1\alpha_1)$. We infer that $h_i \in \mathrm{Ker}(\beta_i)$ $(i = 1, 2)$. Let $a \in A$ with $\varphi_1(a) = h_1$. Then $a \in \mathrm{Ker}(\beta_1\varphi_1) = \mathrm{Ker}(\varphi_1)\mathrm{Ker}(\varphi_2)$. Hence $a = k_1k_2$, where $k_i \in \mathrm{Ker}(\varphi_i)$ $(i = 1, 2)$. Therefore, $h_1 = \varphi_1(k_2)$. Similarly, $h_2 = \varphi_2(l_1)$ for some $l_1 \in \mathrm{Ker}(\varphi_1)$. Thus, $\varphi(l_1k_2) = (h_1, h_2)$. Thus φ is onto. □

The dual concept of pullback is that of pushout. Specifically, a commutative square diagram

$$\begin{array}{ccc} H & \xrightarrow{\beta_1} & H_1 \\ {\scriptstyle\beta_2}\downarrow & & \downarrow{\scriptstyle\alpha_1} \\ H_2 & \xrightarrow[\alpha_2]{} & G \end{array}$$

of profinite groups and continuous homomorphisms is called a *pushout diagram* or a *pushout of β_1 and β_2* if the following universal property is satisfied:



whenever K is a profinite group and $\varphi_i : H_i \longrightarrow K$ $(i = 1, 2)$ are continuous homomorphisms such that $\varphi_1\beta_1 = \varphi_2\beta_2$, then there exists a unique continuous homomorphism $\varphi : G \longrightarrow K$ such that $\varphi\alpha_1 = \varphi_1$ and $\varphi\alpha_2 = \varphi_2$.

The existence of pushout diagrams of profinite groups will be established in Chapter 9.

2.11 Profinite Groups as Galois Groups

In this section we show that profinite groups are precisely those groups that are Galois groups of (finite or infinite) Galois extensions of fields, with an appropriate topology. Historically, this is the original motivation for the study of profinite groups and Galois theory remains the main area of applications of results in profinite groups.

Let K/F be an algebraic, normal and separable extension of fields, that is, a Galois extension. Consider the collection $\mathcal{K} = \{K_i \mid i \in I\}$ of all intermediate subfields $F \subseteq K_i \subseteq K$ such that each K_i/F is a finite Galois extension. Then

$$K = \bigcup_{i \in I} K_i.$$

Let $G = G_{K/F}$ and $U_i = G_{K/K_i}$ denote the Galois groups of K/F and K/K_i $(i \in I)$, respectively. Using elementary results in Galois theory, one sees that

(1) $U_i \triangleleft G$, and $G/U_i \cong G_{K_i/F}$ is finite for every $i \in I$;
(2) If $i, j \in I$, then there exists some $k \in I$ such that $U_k \leq U_i \cap U_j$; and
(3) $\bigcap_{i \in I} U_i = \{1\}$.

Then there is a unique topology on G, compatible with the group structure of G, for which the collection $\{U_i \mid i \in I\}$ is a fundamental system of neighborhoods of the identity element 1 of G (cf. Bourbaki [1989], Ch. III, Proposition 1). This topology is called the *Krull topology* of the Galois group $G = G_{K/F}$. Note that if the Galois extension K/F is finite, then the Krull topology on $G = G_{K/F}$ is the discrete topology.

Theorem 2.11.1 *The Galois group $G = G_{K/F}$, endowed with the Krull topology, is a profinite group. Moreover,*

$$G_{K/F} = \varprojlim_{i \in I} G_{K_i/F}.$$

Proof. For each $i \in I$, consider the finite Galois group $G_i = G_{K_i/F}$. Observe that, with the above notation, $G_i \cong G/U_i$. Define a partial order relation $\preceq$ on the set I as follows. Let $i, j \in I$; then

$i \preceq j$ if $K_i \subseteq K_j$, or equivalently if $U_i = G_{K/K_i} \geq U_j = G_{K/K_j}$. Plainly $(I, \preceq)$ is a poset. In fact it is a directed poset. Indeed, if $K_i, K_j \in \mathcal{K}$, then there exist polynomials $f_i(X), f_j(X) \in F[X]$ such that K_i and K_j are the

splitting fields contained in K of $f_i(X)$ and $f_j(X)$ over F, respectively. Let L be the splitting field over F of the polynomial $f_i(X)f_j(X)$, with $L \subseteq K$. Then $L \in \mathcal{K}$. Say $L = K_t$ for some $t \in I$. Then by definition $t \succeq i, j$.

If $i \preceq j$, define

$$\varphi_{ji} : G_j = G_{K_j/F} \longrightarrow G_i = G_{K_i/F}$$

by restriction, that is, $\varphi_{ji}(\sigma) = \sigma_{|K_i}$, where $\sigma \in G_{K_j/F}$. Observe that φ_{ji} is well-defined, because $\sigma(K_i) = K_i$ since K_i/F is a normal extension. We obtain in this manner an inverse system $\{G_i, \varphi_{ij}, I\}$ of finite Galois groups. Consider the homomorphism

$$\Phi : G = G_{K/F} \longrightarrow \varprojlim_{i \in I} G_i \leq \prod_{i \in I} G_i$$

defined by

$$\Phi(\sigma) = (\sigma_{|K_i}).$$

We shall show that Φ is an isomorphism of topological groups. It is a monomorphism since $\mathrm{Ker}(\Phi) = \bigcap_{i \in I} G_{K_i/F} = 1$. The homomorphism Φ is continuous since the composition

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

is continuous for each $i \in I$. Also, Φ is an open mapping since

$$\Phi(G_{K/K_i}) = (\varprojlim G_i) \cap \left[\left(\prod_{K_j \not\subseteq K_i} G_j \right) \times \left(\prod_{K_j \subseteq K_i} \{1\}_j \right) \right].$$

Finally, Φ is an epimorphism. Indeed, if $(\sigma_i) \in \varprojlim G_i$, define $\sigma : K \longrightarrow K$ by $\sigma(k) = \sigma_i(k)$ for $k \in K_i$; then $\sigma \in G$ and $\Phi(\sigma) = (\sigma_i)$. Thus we have proved that $G \cong \varprojlim G_i$. The result now follows from the characterization of profinite groups obtained in Theorem 2.1.3. □

Example 2.11.2

(1) Let p be a prime number, $\mathbf{F}_p$ the field with p elements, and let $\overline{\mathbf{F}}_p$ be its algebraic closure. Then the Galois group of the extension $\overline{\mathbf{F}}_p/\mathbf{F}_p$ is $\widehat{\mathbf{Z}}$. Indeed, from the theory of finite fields, for each positive integer n, there exists a unique Galois extension $K_n/\mathbf{F}_p$ of degree $[K_n : \mathbf{F}_p] = n$ and $G_{K_n/\mathbf{F}_p} \cong \mathbf{Z}/n\mathbf{Z}$. Thus it follows from Theorem 2.11.1 that

$$G_{\overline{\mathbf{F}}_p/\mathbf{F}_p} = \varprojlim_n \mathbf{Z}/n\mathbf{Z} = \widehat{\mathbf{Z}}.$$

(2) Let p and q be prime numbers. For each positive integer n, there is a unique field L_n with $\mathbf{F}_p \subseteq L_n \subseteq \overline{\mathbf{F}}_p$, such that $[L_n : \mathbf{F}_p] = q^n$. Then $L = \bigcup_{n=1}^{\infty} L_n$ is a Galois extension of $\mathbf{F}_p$, and

$$G_{L/\mathbf{F}_p} = \varprojlim G_{L_n/\mathbf{F}_p} = \varprojlim \mathbf{Z}/q^n\mathbf{Z} = \mathbf{Z}_q.$$

The Krull topology on the Galois group $G = G_{K/F}$ was introduced by Krull [1928]. His aim was to provide a generalization, to infinite Galois extensions, of the Galois correspondence between intermediate fields of (a finite Galois extension) K/F and the subgroups of the group $G_{K/F}$.

Theorem 2.11.3 *Let K/F be a Galois extension of fields with Galois group $G = G_{K/F}$. Denote by $\mathcal{F}(K/F)$ the set of intermediate fields $F \subseteq L \subseteq K$. Endow G with the Krull topology and let $\mathcal{S}(G)$ denote the set of closed subgroups of G. Consider the map*

$$\Phi : \mathcal{F}(K/F) \longrightarrow \mathcal{S}(G)$$

defined by

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

Then Φ is a bijection that reverses inclusion, that is, if $L_1 \subseteq L_2$ are fields in $\mathcal{F}(K/F)$, then $\Phi(L_1) \geq \Phi(L_2)$. The inverse of Φ is the map

$$\Psi : \mathcal{S}(G) \longrightarrow \mathcal{F}(K/F)$$

given by

$$\Psi(H) = \{x \in K \mid \sigma(x) = x, \forall \sigma \in H\}.$$

Moreover, $L \in \mathcal{F}(K/F)$ is a normal extension of F if and only if $\Phi(L)$ is a normal subgroup of G, and if that is the case, $G_{L/F} \cong G/\Phi(L)$.

Proof. It is clear that $\Phi(L)$ reverses inclusion. Observe that $\Phi(L) = G_{K/L}$; furthermore, the Krull topology on $G_{K/L}$ is the topology induced from $G = G_{K/F}$, and since, according to Theorem 2.11.1, $G_{K/L}$ is compact, then it is closed in G; therefore $\Phi(L) \in \mathcal{S}(G)$. Next, we check that $\Psi\Phi(L) = L$ for all $L \in \mathcal{F}(K/F)$. Obviously $\Psi\Phi(L) = \Psi(G_{K/L}) \supseteq L$. Finally, if $y \in K$ and y is fixed by every automorphism $\sigma \in G_{K/L}$, then the minimal polynomial of y over L must be of degree 1; so $y \in L$.

Conversely, let us show that $\Phi\Psi(H) = H$ for every closed subgroup H of G. Put $L = \Psi(H)$. Plainly, $\Phi\Psi(H) = G_{K/L} \supseteq H$. To see that $G_{K/L} = H$, it will suffice to show that H is dense in $G_{K/L}$, since H is closed. Now, let N be an intermediate extension of K/L such that N/L is a finite Galois extension. Let $\tau \in G_{K/L}$; we need to show that $\tau G_{K/N} \cap H \neq \emptyset$. Remark that if $\sigma \in H$, then $\sigma(N) = N$, so $\{\sigma_{|N} \mid \sigma \in H\}$ is a group of automorphisms of N fixing the elements of L; hence, by the fundamental theorem of Galois theory for finite field extensions (cf. Bourbaki [1967], V,10,5, Theorem 3),

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

Then there exists some $\sigma \in H$ such that $\tau_{|N} = \sigma_{|N}$; therefore, $\sigma \in \tau G_{K/N}$, as desired.

Assume now that $L \in \mathcal{F}(K/F)$ and L/F is a normal extension. Let $\sigma \in G_{K/L}, \tau \in G_{K/F}$. Evidently, $\tau^{-1}\sigma\tau \in G_{K/L}$ and so $\Phi(L) = G_{K/L} \triangleleft G_{K/F} = G$. Recall that every F-automorphism of L can be extended to an F-automorphism of K (cf. Bourbaki [1967], V,6,3, Proposition 7). On the other hand, if L/F is normal, then $\tau(L) = L$, for all $\tau \in G = G_{K/F}$. Therefore there is a natural epimorphism

$$G = G_{K/F} \longrightarrow G_{L/F}$$

given by restriction $\tau \mapsto \tau_{|L}$. The kernel of this epimorphism is $\Phi(L) = G_{K/L}$; thus $G_{L/F} \cong G/\Phi(L)$.

Conversely, if $\Phi(L) = G_{K/L} \triangleleft G_{K/F} = G$, it follows that $\tau(L) = L$ for each $\tau \in G = G_{K/F}$. This implies that L/F is a normal extension (cf. Bourbaki [1967], V,6,3, Proposition 6). □

Exercise 2.11.4 Let p be a prime number. Let $\mathbf{F}_p$ be the field with p elements, and $\overline{\mathbf{F}}_p$ its algebraic closure. Prove that the Galois group $G_{\overline{\mathbf{F}}_p/\mathbf{F}_p} \cong \widehat{\mathbf{Z}}$ is topologicaly generated by the Frobenius automorphism $\varphi : \overline{\mathbf{F}}_p \longrightarrow \overline{\mathbf{F}}_p$ given by $\varphi(x) = x^p$. Exhibit explicitly a nonclosed subgroup H of $G_{\overline{\mathbf{F}}_p/\mathbf{F}_p}$ whose fixed field is $\mathbf{F}_p$ (the fixed field of $G_{\overline{\mathbf{F}}_p/\mathbf{F}_p}$).

As we have seen in Theorem 2.11.1, every Galois group can be interpreted as a profinite group. In the next theorem we show that, conversely, every profinite group can be realized as a Galois group of an appropriate Galois extension of fields.

Theorem 2.11.5 *Let G be a profinite group. Then there exists a Galois extension of fields K/L such that $G = G_{K/L}$.*

Proof. Let F be any field. Denote by T the disjoint union of all the sets G/U, where U runs through the collection of all open normal subgroups of G. Think of the elements of T as indeterminates, and consider the field $K = F(T)$ of all rational functions on the indeterminates in T with coefficients in F. The group G operates on T in a natural manner: if $\gamma \in G$ and $\gamma' U \in G/U$, then $\gamma(\gamma' U) = \gamma\gamma' U$. This in turn induces an action of G on K as a group of F-automorphisms of K. Put $L = K^G$, the subfield of K consisting of the elements of K fixed by all the automorphisms $\gamma \in G$. We shall show that K/L is a Galois extension with Galois group G.

If $k \in K$, consider the subgroup

$$G_k = \{\gamma \in G \mid \gamma(k) = k\}$$

of G. If the indeterminates that appear in the rational expression of k are $\{t_i \in G/U_i \mid i = 1, \ldots, n\}$, 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 $U \lhd_o H$ and let K^U be the subfield of the elements fixed by U; then K^U/L is a finite Galois extension by Theorem 2.11.3; say, $K^U = L(k'_1, \ldots, k'_s)$ for some $k'_1, \ldots, k'_s \in K$. Then

$$G \cap U \supseteq \bigcap_{i=1}^{s} G_{k'_i}.$$

Therefore $G \cap U$ is open in G. This shows that G is a closed subgroup of H. Finally, since G and H fix the same elements of K, it follows from Theorem 2.11.3 that $G = H$. □

2.12 Notes, Comments and Further Reading

As pointed out in Section 2.11, interest about general profinite groups appeared first among algebraic number theorists. Krull [1928] defined a natural topology on the Galois group $G_{K/F}$ (usually called now the Krull topology) with the idea of making precise the generalization of the fundamental theorem of Galois theory in the case of extensions of infinite degree (see Theorem 2.11.3). With this topology the Galois group becomes a profinite group (see Theorem 2.11.1).

Profinite groups were first called 'groups of Galois type'; the first systematic presentation of these groups appeared in the influential book Cohomologie Galoisienne by Serre [1995] whose first edition is of 1964; this book has served as a source of information and inspiration to mathematicians, including the authors of the present book, since then. In this book Serre refers to these groups as 'profinite' and 'pro-p' groups to the exclusion of any other terminology. Serre's book contains a systematic use of properties of profinite and pro-p groups to field theory. It is a short volume, written in a very terse style, that contains a wealth of results and information. Books published later

by Poitou [1967], Koch [1970], Ribes [1970], Shatz [1972], Fried and Jarden [2008] and most recently, Dixon, du Sautoy, Mann and Segal [1999], Klaas, Leedham-Green and Plesken [1997], Wilson [1998] concentrate on special aspects of the theory, and are generally more detailed. Serre's book is the best source for certain material, e.g., nonabelian cohomology and applications to field theory.

Some particular profinite groups have a much older history, also rooted in number theory. The group $\mathbf{Z}_p$ of p-adic integers was first defined by Hensel during his studies of algebraic numbers; see Hensel [1908]. Theorem 2.11.5 was first proved by Leptin [1955]; see also Waterhouse [1972]. The proof of this theorem that we present here is taken from Ribes [1977].

Proposition 2.2.2, Exercise 2.2.3, Corollary 2.3.6 and Proposition 2.4.4 appear in Douady [1960], where they are attributed to Tate. Many of the basic results about profinite groups, including cohomological ones, were first established by Tate, but he has not published much on the subject; see Lang [1966], Tate [1962]. See also Appelgate and Onishi [1977], Borovik, Pyber and Shalev [1996], Brauer [1969]. The notion of 'supernatural number' is due to Steinitz [1910], page 250; he uses instead the term 'G-number', but we have decided to stay with the terminology of 'supernatural' because it is well-entrenched by now in the literature and because it is very expressive.

Corollary 2.3.7 can be found in Bolker [1963]. Exercise 2.3.14 appears in Gilotti, Ribes and Serena [1999]; this paper contains results relating to fusion and transfer in the context of profinite groups. Exercise 2.3.17 appears in Lim [1973a]. For a study of localization in profinite groups see Herfort and Ribenboim [1984].

Proposition 2.5.4 was proved in Gaschütz [1956] for finite groups. The proof that we give here is attributed to Roquette in Fried and Jarden [2008]. Corollary 2.6.6 is due to Iwasawa [1953]. See Joly [1965], for a study of procyclic groups. The basic properties of the Frattini subgroup in the context of profinite groups are given in Gruenberg [1967]. Propositions 2.8.2(c) and 2.8.11 appear in Oltikar and Ribes [1978]. Proposition 2.8.9 was proved by Lubotzky [1982]. Lemma 2.8.15 and the concept of Frattini cover can be found in Cossey, Kegel and Kovács [1980]; for additional information on results and applications of Frattini covers, see Ershov [1980], Ershov and Fried [1980], Haran and Lubotzky [1983], Cherlin, van den Dries and Macintyre [1984], Ribes [1985]. For a result on direct products, see Goldstein and Guralnick [2006].

2.12.1 Analytic Pro-p Groups

Let G be a finitely generated profinite group. According to Proposition 2.5.5, every open subgroup U of G is also finitely generated. However the minimal number $d(U)$ of generators of U is usually unbounded (see Theorem 3.6.2(b) for the case of free profinite groups). More generally, if H is a closed subgroup of G, then one can usually say little about $d(H)$. Nevertheless, there is

an important class of finitely generated profinite groups G for which

$$\max\{d(H) \mid H \leq_c G\} = r(G) < \infty.$$

(The number $r(G)$ thus defined is sometimes called the 'rank' of the group G; we refrain from this terminology to avoid confusion with the concept of rank of a free group which will be introduced in Chapter 3.)

A representative example of such groups is $G = \mathrm{GL}_n(\mathbf{Z}_p)$. This group contains an open pro-p subgroup K_1 of index $(p^n - 1)(p^{n-1} - 1)\cdots(p-1)$ (see Exercise 2.3.12). One can then prove the following result (see, e.g., Dixon, du Sautoy, Mann and Segal [1999], Theorem 5.2):

Theorem 2.12.1a $r(K_1) = n^2$. *Consequently,* $r(G) < \infty$.

Profinite groups satisfying conditions analogous to those mentioned above for $\mathrm{GL}_n(\mathbf{Z}_p)$ are called *p-adic analytic groups*. Explicitly, a profinite group G is p-adic analytic if it contains an open pro-p subgroup H such that $r(H) < \infty$. The reason for this terminology is the following theorem due to Lazard (see Lazard [1965], III, 3.4). Let $\mathbf{Q}_p$ be the field of p-adic numbers, that is, the field of quotients of $\mathbf{Z}_p$.

Theorem 2.12.1b *Let G be a Hausdorff topological group. Then G is p-adic analytic if and only if G is compact and admits a structure of a $\mathbf{Q}_p$-manifold in such a way that multiplication and inversion in G are analytic functions.*

Research in the theory of profinite p-adic analytic groups and related topics is presently very active. An excellent modern exposition can be found in Dixon, du Sautoy, Mann and Segal [1999]. See also Lazard [1965, 1954] (these two works contain a large amount of information on these and other topics rarely found elsewhere), Lubotzky and Mann [1989], Lubotzky and Segal [2003], Mann and Segal [1990], du Sautoy [1993], du Sautoy and Grunewald [2002], Fernández-Alcober, González-Sánchez and Jaikin-Zapirain [2008], Shalev [1992]. See also Detomi and Lucchini [2007].

2.12.2 Number of Generators of a Group and of Its Profinite Completion

Let G be a finitely generated residually finite abstract group and consider its profinite completion $\widehat{G}$. We denote by $d(G)$ the minimal cardinality of a set of generators of G as an abstract group; while $d(\widehat{G})$ denotes the minimal cardinality of a set of generators of $\widehat{G}$ as a profinite group. Obviously $d(\widehat{G}) \leq d(G)$. Put $f(G) = d(G) - d(\widehat{G})$. Then one has the following results.

Theorem 2.12.2a (Noskov [1983]) *For each natural number n, there exist a finitely generated abstract metabelian group G_n such that $f(G_n) \geq n$.*

On the other hand, for polycyclic groups G one has

Theorem 2.12.2b (Linnell and Warhurst [1981]) *If G is a polycyclic group, then $f(G) \leq 1$.*