Dinakar Ramakrishnan
Robert J. Valenza

Fourier Analysis on Number Fields

Springer

1 Topological Groups

Our work begins with the development of a topological framework for the key elements of our subject. The first section introduces the category of topological groups and their fundamental properties. We treat, in particular, uniform continuity, separation properties, and quotient spaces. In the second section we narrow our focus to locally compact groups, which serve as the locale for the most important mathematical phenomena treated subsequently. We establish the essential deep feature of such groups: the existence and uniqueness of Haar measure; this is fundamental to the development of abstract harmonic analysis. The last two sections further specialize to profinite groups, giving a topological characterization, a structure theorem, and a set of results roughly analogous to the Sylow Theorems for finite groups. The prerequisites for this discussion will be found in almost any first-year graduate courses in algebra and analysis.

1.1 Basic Notions

DEFINITION. A *topological group* is a group G (identity denoted e) together with a topology such that the following conditions hold:

(i) The group operation

$$\begin{aligned} G\times G &\to G \\ (g,h) &\mapsto gh \end{aligned}$$

is a continuous mapping. (The domain has the product topology.)

(ii) The inversion map

$$\begin{aligned} G &\to G \\ g &\mapsto g^{-1} \end{aligned}$$

is likewise continuous.

By convention, whenever we speak of a finite topological group, we intend the discrete topology.

Clearly the class of topological groups together with continuous homomorphisms constitutes a category.

It follows at once that translation (on either side) by any given group element is a homeomorphism $G \to G$. Thus the topology is *translation invariant* in the sense that for all $g \in G$ and $U \subseteq G$ the following three assertions are equivalent:

(i) U is open.

(ii) gU is open.

(iii) Ug is open.

Moreover, since inversion is likewise a homeomorphism, U is open if and only if $U^{-1} = \{x : x^{-1} \in U\}$ is open.

A fundamental aspect of a topological group is its *homogeneity*. In general, if X is any topological space, Homeo(X) denotes the set of all homeomorphisms $X \to X$. If S is a subset of Homeo(X), then one says that X is a *homogeneous space under* S if for all $x, y \in X$, there exists $f \in S$ such that $f(x)=y$. (When S is unspecified or perhaps all of Homeo(X), one says simply that X is a *homogeneous space*.) Clearly any topological group G is homogeneous under itself in the sense that given any points $g, h \in G$, the homeomorphism defined as left translation by hg^{-1} (i.e., $x \mapsto hg^{-1}x$) sends g to h. From this it follows at once that a local base at the identity $e \in G$ determines a local base at any point in G, and in consequence the entire topology.

EXAMPLES

(1) Any group G is a topological group with respect to the discrete topology.

(2) $\mathbf{R}^*$, $\mathbf{R}^*_+$, and $\mathbf{C}^*$ are topological groups with respect to ordinary multiplication and the Euclidean topology.

(3) $\mathbf{R}^n$ and $\mathbf{C}^n$ are topological groups with respect to vector addition and the Euclidean topology.

(4) Let $k = \mathbf{R}$ or $\mathbf{C}$. Then the general linear group

$$\mathrm{GL}_n(k) = \{g \in M_n(k) : \det(g) \neq 0\} \quad (n \geq 1)$$

is a topological group with respect to matrix multiplication and the Euclidean topology. The special linear group

$$\mathrm{SL}_n(k) = \{g \in \mathrm{GL}_n(k) : \det(g) = 1\} \quad (n \geq 1)$$

is a closed subgroup of $\mathrm{GL}_n(k)$.

In subsequent discussion, if X is a topological space and $x \in X$, we shall say that $U \subseteq X$ is a *neighborhood of* x if x lies in the interior of U (i.e., the largest open subset contained in U). Thus a neighborhood need not be open, and it makes sense to speak of a closed or compact neighborhood, as the case may be.

A subset S of G is called *symmetric* if $S = S^{-1}$. This is a purely group-theoretic concept that occurs in the following technical proposition.

1-1 PROPOSITION. *Let G be a topological group. Then the following assertions hold:*

(i) *Every neighborhood U of the identity contains a neighborhood V of the identity such that $VV \subseteq U$.*

(ii) *Every neighborhood U of the identity contains a symmetric neighborhood V of the identity.*

(iii) *If H is a subgroup of G, so is its closure.*

(iv) *Every open subgroup of G is also closed.*

(v) *If K_1 and K_2 are compact subsets of G, so is K_1K_2.*

PROOF. (i) Certainly we may assume that U is open. Consider the continuous map $\varphi: U \times U \to G$ defined by the group operation. Certainly $\varphi^{-1}(U)$ is open and contains the point (e,e). By definition of the topology on $U \times U$, there exist open subsets V_1, V_2 of U such that $(e,e) \in V_1 \times V_2$. Set $V = V_1 \cap V_2$. Then V is a neighborhood of e contained in U such that by construction $VV \subseteq U$. $V_1 \times V_2 \subseteq \varphi^{-1}(U$

(ii) Clearly $g \in U \cap U^{-1} \Leftrightarrow g, g^{-1} \in U$, so $V = U \cap U^{-1}$ is the required symmetric neighborhood of e.

(iii) Any two points g and h in the closure of H may be exhibited as the limits of convergent nets in H itself. Hence by continuity their product is likewise the limit of a convergent net in H and similarly for inverses.

(iv) If H is any subgroup of G, then G is the disjoint union of the cosets of H, and hence H itself is the complement of the union of its nontrivial translates. If H is open, so are these translates, whence H is the complement of an open set and therefore closed.

(v) K_1K_2 is the image of the compact set $K_1 \times K_2$ under the continuous map $(k_1, k_2) \mapsto k_1k_2$. It is therefore compact by general topology □

Note that (i) and (ii) together imply that every neighborhood U of the identity contains a symmetric neighborhood V such that $VV \subseteq U$.

Translation of Functions and Uniform Continuity

Given an arbitrary function f on a group, we define its *left* and *right translates* by the formulas

$$L_hf(g)=f(h^{-1}g) \quad \text{and} \quad R_hf(g)=f(gh) \ .$$

If f is a (real- or complex-valued) continuous function on a topological group, we say that f is *left uniformly continuous* if for every $\varepsilon>0$ there is a neighborhood V of e such that

$$h \in V \Rightarrow \| L_hf - f \|_u < \varepsilon$$

where $\| \ \|_u$ denotes the uniform, or sup, norm. Right uniform continuity is defined similarly. Recall that $\mathscr{C}_c(G)$ denotes the set of continuous functions on G with compact support.

1-2 Proposition. *Let G be a topological group. Then every function f in $\mathscr{C}_c(G)$ is both left and right uniformly continuous.*

Proof. We prove right uniform continuity. Let $K=\text{supp}(f)$ and fix $\varepsilon>0$. Then for every $g\in K$ there exists an open neighborhood U_g of the identity such that

$$h \in U_g \Rightarrow |f(gh) - f(g)| < \varepsilon \ .$$

Equivalently, $f(g')$ is ε-close to $f(g)$ whenever $g^{-1}g'$ lies in U_g. Moreover, by the comment following the previous proposition, each U_g contains an open symmetric neighborhood V_g of the identity such that $V_gV_g\subseteq U_g$. Clearly the collection of subsets gV_g covers K, and a finite subcollection $\{g_jV_j\}_{j=1,\dots,n}$ suffices. Henceforth we write V_j for V_{g_j} and U_j for U_{g_j}. Define V, a symmetric open neighborhood of the identity e, by the formula

$$V = \bigcap_{j=1}^{n} V_j \ .$$

If $g\in K$, then $g\in g_jV_j$ for some j. For $h\in V$ we consider the difference $f(gh)-f(g)$:

$$|f(gh) - f(g)| \le |f(gh) - f(g_j)| + |f(g_j) - f(g)| \ .$$

The point is that both $g_j^{-1}g$ and $g_j^{-1}gh$ lie in U_j, so that both terms on the right are bounded by ε. (Here is where we use that property $V_jV_j\subseteq U_j$ for all j.) This establishes right uniform continuity for K.

When g does not lie in K, then we must bound $|f(gh)|$. If $f(gh)\neq 0$, then $gh\in g_jV_j$ for some j, and therefore $f(gh)$ is ε-close to $f(g_j)$. Moreover, $g_j^{-1}g=g_j^{-1}ghh^{-1}$ lies in U_j (here is where we use the symmetry of V), and it follows that $|f(g_j)|<\varepsilon$ since g_j is close to g and $f(g)=0$ by assumption. Consequently $|f(gh)|<2\varepsilon$, and the argument is complete. □

Separation Properties and Quotient Spaces

Some authors assume as part of the definition of a topological group that the underlying topology is T_1. In this case it is also customary to reserve the term *subgroup* for a closed subset that constitutes a subgroup in the ordinary algebraic sense. Note that in general we accept neither of these assumptions.

The following proposition shows, among other things, that for a topological group the separation axioms T_1 and T_2 (Hausdorff) have equal strength.

1-3 Proposition. *Let G be a topological group. Then the following assertions are equivalent:*

(i) *G is T_1.*

(ii) *G is Hausdorff.*

(iii) *The identity e is closed in G.*

(iv) *Every point of G is closed.*

Proof. (i)$\Rightarrow$(ii) If G is T_1, then for any distinct $g,h\in G$ there is an open neighborhood U of the identity lacking gh^{-1}. According to Proposition 1-1, U admits a symmetric open subset V, also containing the identity, such that $VV\subseteq U$. Then Vg and Vh are disjoint open neighborhoods of g and h, since otherwise gh^{-1} lies in $V^{-1}V=VV\subseteq U$.

(ii)$\Rightarrow$(iii) Every point in a Hausdorff (or merely T_1) space is closed.

(iii)$\Rightarrow$(iv) This is a consequence of homogeneity: For every point $x\in G$ there is a homeomorphism that carries e onto x. Hence if e is closed, so is every point.

(iv)$\Rightarrow$(i) Obvious by general topology. □

If H is a subgroup of the topological group G, then the set G/H of left cosets of G acquires the *quotient topology*, defined as the strongest topology such that the canonical projection $\rho{:}\,g\mapsto gH$ is continuous. Thus U is open in G/H if and only if $\rho^{-1}(U)$ is open in G. Recall from algebra that G/H constitutes a group under coset multiplication if and only if H is moreover normal in G. We shall see shortly that in this case G/H also constitutes a topological group with respect to the quotient topology.

The following two propositions summarize some of the most important properties of the quotient construction.

1-4 Proposition. *Let G be a topological group and let H be a subgroup of G. Then the following assertions hold:*

(i) *The quotient space G/H is homogeneous under G.*

(ii) *The canonical projection $\rho: G \to G/H$ is an open map.*

(iii) *The quotient space G/H is T_1 if and only if H is closed.*

(iv) *The quotient space G/H is discrete if and only if H is open. Moreover, if G is compact, then H is open if and only if G/H is finite.* (and discrete)

(v) *If H is normal in G, then G/H is a topological group with respect to the quotient operation and the quotient topology.*

(vi) *Let H be the closure of $\{e\}$ in G. Then H is normal in G, and the quotient group G/H is Hausdorff with respect to the quotient topology.*

Proof. (i) An element $x \in G$ acts on G/H by left translation: $gH \mapsto xgH$. The inverse map takes the same form, so to show that left translation is a homeomorphism of G/H, it suffices to show that left translation is an open mapping on the quotient space. Let $\overline{U}$ be an open subset of G/H. By definition of the quotient topology, the inverse image of $\overline{U}$ under ρ is an open subset U of G, and it follows that the inverse image of $g\overline{U}$ under ρ is gU, also an open subset of G. Therefore $g\overline{U}$ is open, and left translation is indeed an open map, as required.

(ii) Let V be an open subset of G. We must show that $\rho(V)$ is open in the quotient. But $\rho(V)$ is open in G/H if and only if $\rho^{-1}(\rho(V))$ is open in G. By elementary group theory, $\rho^{-1}(\rho(V)) = V \cdot H$. Let x lie in $V \cdot H$, so that $x = vh$ for some $v \in V$ and $h \in H$. Since V is open, given any $v \in V$, there is an open neighborhood $U_v \subseteq V$ containing v. Thus $U_v \cdot h$ is an open neighborhood of x contained in $V \cdot H$, which is accordingly open.

(iii) By general topology, G/H is T_1 if and only if every point is closed. Since a coset of H is its own inverse image under projection, each coset is a closed point in G/H if and only if each is likewise a closed subset of G. But by homogeneity this is the case if and only if H itself is closed in G. (Note that we cannot appeal to the previous proposition, since the topological space G/H is not necessarily a topological group with respect to multiplication of cosets.)

(iv) Let H be a subgroup of G. Then by part (ii), H is an open subset of G if and only if H is an open point of G/H. Since G/H is homogeneous under G, this holds if and only if G/H is discrete. Assume now that G is compact. Then so is G/H, since ρ is continuous. But then H is open if and only if G/H is both compact and discrete, which is to say, if and only if G/H is finite. (Recall our convention that a finite topological group carries the discrete topology.)

(v) Assume that H is a normal subgroup of G. Then from part (ii) and the commutative diagram

$$\begin{tikzcd}
G \arrow[r, "T_g"] \arrow[d, "\rho"'] & G \arrow[d, "\rho"] \\
G/H \arrow[r, "T_{\rho(g)}"] & G/H
\end{tikzcd}$$

(where T_g denotes left translation by g), we see at once that translation by any group element is continuous on the quotient. A similar diagram establishes the continuity of the inversion map.

(vi) Since $\{e\}$ is a subgroup of G, so is its closure H. Moreover, it is the smallest closed subgroup of G containing e and therefore normal, since each conjugate of H is likewise a closed subgroup containing e. In light of the previous proposition, the full assertion now follows from parts (iii) and (v) above. ❑

Part (vi) shows that every topological group projects by a continuous homomorphism onto a topological group with Hausdorff topology. In this sense the assumption that a given group is Hausdorff is not too serious.

1-5 Proposition. *Let G be a Hausdorff topological group. Then the following assertions hold:*

(i) *The product of a closed subset F and a compact subset K is closed.*

(ii) *If H is a compact subgroup of G, then $\rho: G \to G/H$ is a closed map.*

Proof. (i) Let z lie in the closure of the product FK. Then there exists a net converging to z of the form $\{x_\alpha y_\alpha\}$ with $x_\alpha \in F$ and $y_\alpha \in K$. Since K is compact, we may replace our given net by a subnet such that $\{y_\alpha\}$ converges to some point y in K. We claim that this forces the convergence of $\{x_\alpha\}$ in F to zy^{-1}, showing that $z = zy^{-1}y$ lies in FK, which is therefore closed. To establish the claim, consider an arbitrary open neighborhood U of the identity e. We may choose yet another neighborhood of e contained in U such that $VV \subseteq U$. Then the nets $\{z^{-1}x_\alpha y_\alpha\}$ and $\{y_\alpha^{-1}y\}$ are both eventually in V, whence the product $z^{-1}x_\alpha y_\alpha y_\alpha^{-1} y = z^{-1}x_\alpha y$ is eventually in U. Thus $\lim x_\alpha = zy^{-1}$, as required.

(ii) If X is a closed subset of G, then arguing as the second part of the previous proposition, we are reduced to showing that $X{\cdot}H$ is likewise a closed subset of G. But if H is compact, this is just a special case of assertion (i). □

REMARK. The requirement that H be compact is essential. For example, in the case $G=\mathbf{R}^2$, with subgroup $H=\{(0,y):y\in\mathbf{R}\}$, we have clearly $G/H\cong\mathbf{R}$, and under this identification, $\rho(x,y)=x$. Now let $X=\{(x,y)\in\mathbf{R}^2 : xy=1\}$. Then X is closed, but $\rho(X)=\mathbf{R}^*$ is not.

Locally Compact Groups

Recall that a topological space is called *locally compact* if every point admits a compact neighborhood.

DEFINITION. A topological group G that is both locally compact and Hausdorff is called a *locally compact group*.

Note well the assumption that a locally compact group is Hausdorff. Accordingly, all points are closed.

1-6 PROPOSITION. *Let G be a Hausdorff topological group. Then a subgroup H of G that is locally compact (in the subspace topology) is moreover closed. In particular, every discrete subgroup of G is closed.*

PROOF. Let K be a compact neighborhood of e in H. Then K is closed in H, since H is likewise Hausdorff, and therefore there exists a closed neighborhood U of e in G such that $K=U\cap H$. Since $U\cap H$ is compact in H, it is also compact in G, and therefore also closed. By Proposition 1-1, part (i), there exists a neighborhood V of e in G such that $VV\subseteq U$. We shall now show that $x\in\overline{H}\Rightarrow x\in H$.

First note that $\overline{H}$ is a subgroup of G by Proposition 1-1, part (iii). Thus if $x\in\overline{H}$, then every neighborhood of x^{-1} meets H. In particular, there exists some $y\in Vx^{-1}\cap H$. We claim that the product yx lies in $U\cap H$. Granting this, both y and yx lie in the subgroup H, whence so does x, as required.

PROOF OF CLAIM. Since $U\cap H$ is closed, it suffices to show that every neighborhood W of yx meets $U\cap H$. Since $y^{-1}W$ is a neighborhood of x, so is $y^{-1}W\cap xV$. Moreover, by assumption x lies in the closure of H, so there exists some element $z\in y^{-1}W\cap xV\cap H$. Now consider:

(i) the product yz lies both in W and in the subgroup H;

(ii) by construction, $y\in Vx^{-1}$;

(iii) by construction, $z\in xV$.

The upshot is that yz lies in $Vx^{-1}\cdot xV=VV$, a subset of U, and therefore the intersection $W\cap(U\cap H)$ is nonempty. This establishes the claim and thus completes the proof. □

1.2 Haar Measure

We first recall a sequence of fundamental definitions from analysis that culminate in the definition of a Haar measure. We shall then establish both its existence and uniqueness for locally compact groups.

A collection $\mathfrak{M}$ of subsets of a set X is called a *σ-algebra* if it satisfies the following conditions:

(i) $X\in\mathfrak{M}$.

(ii) If $A\in\mathfrak{M}$, then $A^c\in\mathfrak{M}$, where A^c denotes the complement of A in X.

(iii) Suppose that $A_n\in\mathfrak{M}$ $(n\geq 1)$, and let

$$A=\bigcup_{n=1}^{\infty}A_n\ .$$

Then also $A\in\mathfrak{M}$; that is, $\mathfrak{M}$ is closed under countable unions.

It follows from these axioms that the empty set is in $\mathfrak{M}$ and that $\mathfrak{M}$ is closed under finite and countably infinite intersections.

A set X together with a σ-algebra of subsets $\mathfrak{M}$ is called a *measurable space*. If X is moreover a topological space, we may consider the smallest σ-algebra $\mathscr{B}$ containing all of the open sets of X. The elements of $\mathscr{B}$ are called the *Borel subsets* of X.

A *positive measure* μ on an arbitrary measurable space $\langle X,\mathfrak{M}\rangle$ is a function $\mu:\mathfrak{M}\to\mathbf{R}_+\cup\{\infty\}$ that is *countably additive*; that is,

$$\mu(\bigcup_{n=1}^{\infty}A_n)=\sum_{n=1}^{\infty}\mu(A_n)$$

for any family $\{A_n\}$ of disjoint sets in $\mathfrak{M}$. In particular, a positive measure defined on the Borel sets of a locally compact Hausdorff space X is called a *Borel measure*.

Let μ be a Borel measure on a locally compact Hausdorff space X, and let E be a Borel subset of X. We say that μ is *outer regular* on E if

$$\mu(E)=\inf\{\mu(U):U\supseteq E,\ U\text{ open}\}\ .$$

We say that μ is *inner regular* on E if

$$\mu(E) = \sup\{\mu(K) : K \subseteq E,\ K \text{ compact}\} \ .$$

A *Radon measure* on X is a Borel measure that is finite on compact sets, outer regular on all Borel sets, and inner regular on all open sets. One can show that a Radon measure is, moreover, inner regular on σ-finite sets (that is, countable unions of μ-measurable sets of finite measure).

Let G be a group and let μ be a Borel measure on G. We say that μ is *left translation invariant* if for all Borel subsets E of G,

$$\mu(sE) = \mu(E)$$

for all $s \in G$. *Right translation invariance* is defined similarly.

Definition. Let G be a locally compact topological group. Then a *left* (respectively, *right*) *Haar measure* on G is a nonzero Radon measure μ on G that is left (respectively, right) translation-invariant. A *bi-invariant Haar measure* is a nonzero Radon measure that is both left and right invariant.

The following proposition shows that the existence of a left Haar measure is equivalent to the existence of a right Haar measure and, in a sense, equates the translation invariance of measure with that of integration. As usual, we let

$$\mathscr{C}_c^+(G) = \{f \in \mathscr{C}_c(G) : f(s) \geq 0 \ \forall s \in G \text{ and } \|f\|_u > 0\} \ .$$

We often abbreviate this to $\mathscr{C}_c^+$ when the domain is clear.

1-7 Proposition. *Let G be a locally compact group with nonzero Radon measure μ. Then:*

(i) *The measure μ is a left Haar measure on G if and only if the measure $\tilde{\mu}$ defined by $\tilde{\mu}(E) = \mu(E^{-1})$ is a right Haar measure on G.*

(ii) *The measure μ is a left Haar measure on G if and only if*

$$\int_G L_s f \, d\mu = \int_G f \, d\mu$$

for all $f \in \mathscr{C}_c^+$ and $s \in G$.

(iii) *If μ is a left Haar measure on G, then μ is positive on all nonempty open subsets of G and*

$$\int_G f \, d\mu > 0$$

for all $f \in \mathscr{C}_c^+$.

(iv) *If μ is a left Haar measure on G, then $\mu(G)$ is finite if and only if G is compact.*

Proof. (i) By definition, we have the equivalence

$$\tilde{\mu}(E) = \tilde{\mu}(Es) \ \forall s \in G \iff \mu(E^{-1}) = \mu(s^{-1}E^{-1}) \ \forall s \in G$$

for all Borel sets E; the assertion follows at once. (For *any* topological group G, clearly E is a Borel subset of G if and only if E^{-1} is.)

(ii) If μ is a Haar measure on G, then the stated equality of integrals follows by definition for all simple functions $f \in \mathscr{C}_c^+$ (i.e., finite linear combinations of characteristic functions on G), and hence, by taking limits, for arbitrary $f \in \mathscr{C}_c^+$. Conversely, from the positive linear functional $\int_G \cdot \, d\mu$ on $\mathscr{C}_c(G)$ we can, by the Riesz representation theorem, explicitly recover the Radon measure μ of any open subset $U \subseteq G$ as follows:

$$\mu(U) = \sup\{\int_G f \, d\mu : f \in \mathscr{C}_c(G),\ \|f\|_u \leq 1, \text{ and } \operatorname{supp}(f) \subseteq U\} \ .$$

From this one sees at once that if the integral is left translation invariant, then $\mu(sU) = \mu(U)$ for all open subsets U of G, since $\operatorname{supp}(f) \subseteq U$ if and only if $\operatorname{supp}(L_s f) \subseteq sU$. The result now extends to all Borel subsets of G because a Radon measure is by definition outer regular.

(iii) Since μ is not identically 0, by inner regularity there is a compact set K such that $\mu(K)$ is positive. Let U be any nonempty open subset of G. Then from the inclusion

$$K \subseteq \bigcup_{s \in G} sU$$

we deduce that K is covered by a finite set of translates of U, all of which must have equal measure. Thus since $\mu(K)$ is positive, so is $\mu(U)$. If $f \in \mathscr{C}_c^+$, then there exists a nonempty open subset U of G on which f exceeds some positive constant R. It then follows that

$$\int_G f \, d\mu \geq R\mu(U) > 0$$

as claimed.

(iv) If G is compact, then certainly $\mu(G)$ is finite by definition of a Radon measure. To establish the converse, assume that G is not compact. Let K be a compact set whose interior contains e. Then no finite set of translates of K covers G (which would otherwise be compact), and there must exist an infinite sequence $\{s_j\}$ in G such that

$$s_n \notin \bigcup_{j<n} s_j K \quad . \tag{1.1}$$

Now K contains a symmetric neighborhood U of e such that $UU \subseteq K$. We claim that the translates s_jU $(j \geq 1)$ are disjoint, from which it follows at once from (iii) that $\mu(G)$ is infinite.

Proof of Claim. Suppose that for $i<j$ we have $s_iu=s_jv$ where $u,v \in U$. Then $s_j = s_iuv^{-1} \in s_iK$, since U is symmetric and $UU \subseteq K$. But this contradicts Eq. 1.1. □

With these preliminaries completed, we now come to one of the major theorems in analysis.

1-8 Theorem. *Let G be a locally compact group. Then G admits a left (hence right) Haar measure. Moreover, this measure is unique up to a scalar multiple.*

Via the Riesz representation theorem and statement (ii) of the previous proposition, the existence part of the proof reduces to the construction of a left-invariant linear functional on $\mathscr{C}_c(G)$. The key idea is the introduction of a translation-invariant device for comparing functions in $\mathscr{C}_c^+$.

Preliminaries to the Existence Proof

Let $f, \varphi \in \mathscr{C}_c^+$. Set $U=\{s \in G: \varphi(s) > \|\varphi\|_u/2\}$, so that a finite number of translates of the open set U suffice to cover supp(f). Then there are n elements $s_1,\dots,s_n \in G$ such that a linear combination of the translates of φ by the s_j dominates f in the following sense:

$$f \leq \frac{2\|f\|_u}{\|\varphi\|_u} \sum_{j=1}^{n} L_{s_j}\varphi \quad .$$

The point is that if $s \in \text{supp}(f)$, then $s \in s_jU$ for some j, so that $s_j^{-1}s \in U$ if φ is sufficiently large. Thus it makes sense to define $(f\!:\!g)$, *the Haar covering number* of f with respect to φ, by the formula

$$(f\!:\!\varphi) = \inf\left\{\sum_{j=1}^{n} c_j : 0 < c_1,\dots,c_n \text{ and } f \leq \sum_{j=1}^{n} c_j L_{s_j}\varphi \text{ for some } s_1,\dots,s_n \in G\right\} .$$

Note that since $\|f\|_u$ is assumed positive, the Haar covering number is never zero. We shall see shortly that $(f\!:\!\varphi)$ is almost linear in f for appropriately chosen φ.

1-9 Lemma. *The Haar covering number has the following properties:*

(i) $(f\!:\!\varphi) = (L_sf\!:\!\varphi)$ *for all* $s \in G$

(ii) $(f_1+f_2\!:\!\varphi) \leq (f_1\!:\!\varphi) + (f_2\!:\!\varphi)$

(iii) $(cf\!:\!\varphi) = c(f\!:\!\varphi)$ *for any* $c>0$

(iv) $(f_1\!:\!\varphi) \leq (f_2\!:\!\varphi)$ *whenever* $f_1 \leq f_2$

(v) $(f\!:\!\varphi) \geq \|f\|_u/\|\varphi\|_u$

(vi) $(f_1\!:\!\varphi) \leq (f_1\!:\!f_0)(f_0\!:\!\varphi)$

Proof. (i) Since left multiplication by any given group element constitutes a permutation of the ambient group, for all $s \in G$ we have the equivalence

$$f(t) \leq \sum c_jL_{s_j}\varphi(t) \;\; \forall t \in G \Leftrightarrow L_sf(t) \leq \sum c_jL_{ss_j}\varphi(t) \;\; \forall t \in G$$

which is to say that

$$f \leq \sum c_jL_{s_j}\varphi \Leftrightarrow L_sf \leq \sum c_jL_{ss_j}\varphi \quad .$$

Hence precisely the same sets of coefficients c_j occur in the calculation of $(f\!:\!\varphi)$ as for $(L_sf\!:\!\varphi)$.

(ii), (iii), (iv) Obvious.

(v) If the coefficients c_j appear in the calculation of $(f\!:\!\varphi)$, then

$$f(s) \leq \sum c_j\varphi(s_j^{-1}s) \leq (\sum c_j)\|\varphi\|_u \quad \forall s \in G$$

whence $\sum c_j \geq \|f\|_u/\|\varphi\|_u$, and the assertion follows.

(vi) We have the implication

$$f_1 \leq \sum c_jL_{s_j}f_0 \text{ and } f_0 \leq \sum d_kL_{t_k}\varphi \;\; \Rightarrow \;\; f_1 \leq \sum c_jd_kL_{s_jt_k}\varphi$$

whence

$$(f_1{:}\varphi) \le \inf \sum c_j d_k = \inf(\sum c_j)\inf(\sum d_k) = (f_1{:}f_0)(f_0{:}\varphi)$$

as claimed. This completes the proof. □

The Haar covering number yields an "approximate" functional as follows. Fix $f_0 \in \mathscr{C}_c^+$ and define

$$I_\varphi(f) = \frac{(f{:}\varphi)}{(f_0{:}\varphi)} \quad (f, \varphi \in \mathscr{C}_c^+) \ .$$

By (vi) above, we have the inequalities

$$(f{:}\varphi) \le (f{:}f_0)(f_0{:}\varphi) \text{ and } (f_0{:}\varphi) \le (f_0{:}f)(f{:}\varphi) \ .$$

Dividing the first by $(f_0{:}\varphi)$ and the second by $(f{:}\varphi)$, we find that I_φ is bounded as follows:

$$(f_0{:}f)^{-1} \le I_\varphi(f) \le (f{:}f_0) \ . \tag{1.2}$$

This bound is crucial to the existence of a Haar measure for G.

One would expect that as the support of φ shrinks, I_φ will become more nearly linear. This is confirmed by the following lemma.

1-10 LEMMA. *Given f_1 and f_2 in $\mathscr{C}_c^+$, for every $\varepsilon>0$ there is a neighborhood V of the identity e such that*

$$I_\varphi(f_1) + I_\varphi(f_2) \le I_\varphi(f_1+f_2) + \varepsilon$$

whenever the support of φ lies in V.

PROOF. By Urysohn's lemma for locally compact Hausdorff spaces, there exists a function $g \in \mathscr{C}_c^+$ that takes the value 1 on $\text{supp}(f_1+f_2) = \text{supp}(f_1) \cup \text{supp}(f_2)$. Choose $\delta>0$ and let $h = f_1 + f_2 + \delta g$, so that h is continuous. Next let $h_i = f_i/h$, $i=1,2$, with the understanding that h_i is 0 off the support of f_i. Clearly both h_i lie in $\mathscr{C}_c^+$, and their sum approaches 1 from below as δ tends to 0. By uniform continuity, there exists a neighborhood U of e such that $|h_i(s)-h_i(t)| < \delta$ whenever $t^{-1}s \in U$.

Assume that $\text{supp}(\varphi)$ lies in U and suppose that

$$h \le \sum_j c_j L_{s_j} \varphi \ .$$

Then

$$f_i(s) = h(s)h_i(s) \le \sum_j c_j \varphi(s_j^{-1}s)h_i(s) \le \sum_j c_j \varphi(s_j^{-1}s)(h_i(s_j)+\delta) \quad (i=1,2)$$

and it follows that

$$(f_i{:}\varphi) \le \sum_j c_j [h_i(s_j) + \delta] \quad (i=1,2) \ .$$

Since $h_1+h_2 \le 1$, this last inequality implies that

$$(f_1{:}\varphi) + (f_2{:}\varphi) \le (1+2\delta)\sum_j c_j \ .$$

But $\sum c_j$ may be made arbitrarily close to $(h{:}\,\varphi)$, and therefore by definition of I_φ and part (ii) of the previous lemma,

$$\begin{aligned} I_\varphi(f_1) + I_\varphi(f_2) &\le (1+2\delta) I_\varphi(h) \\ &\le (1+2\delta)[I_\varphi(f_1+f_2) + \delta I_\varphi(g)] \\ &= I_\varphi(f_1+f_2) + 2\delta[I_\varphi(f_1+f_2) + \delta I_\varphi(g)] \ . \end{aligned}$$

Finally, Eq. 1.2 asserts that all of the I_φ-terms on the right are bounded independently of φ, and so for any positive $\varepsilon>0$ we can choose δ sufficiently small that the stated inequality holds. □

Existence of Haar Measure

We now prove the existence of a Haar measure for a locally compact group G. The idea is to construct from our approximate left-invariant functionals I_φ an exact linear functional. We shall obtain this as a limit in a suitable space.

Let X be the compact topological space defined by the bounds of $I_\varphi(f)$ as follows:

$$X = \prod_{f \in \mathscr{C}_c^+} [(f_0{:}f)^{-1}, (f{:}f_0)] \ .$$

Then every function I_φ (in the technical sense of a set of ordered pairs in $\mathscr{C}_c^+ \times \mathbf{R}_+^*$) lies in X. For every compact neighborhood U of e, let K_U be the closure of the set $\{I_\varphi : \text{supp}(\varphi) \subseteq U\}$ in X. The collection $\{K_U\}$ satisfies the finite intersection property, since

$$\bigcap_{j=1}^{n} K_{U_j} \supseteq K_{\bigcap_{j=1}^{n} U_j}$$

and the right side is nonempty by Urysohn's lemma. Therefore, since X is compact, $\bigcap K_U$ contains an element I, which will in fact extend to the required left-invariant positive linear functional on $\mathscr{C}_c(G)$. Note that I, which lies in a product of closed intervals excluding zero, cannot be the zero function on $\mathscr{C}_c(G)$, so that the extended functional will likewise be nontrivial.

Since I is in the intersection of the closure of the sets $\{I_\varphi : \text{supp}(\varphi) \subseteq U\}$, it follows that every open neighborhood of I in the product X intersects each of the sets $\{I_\varphi : \text{supp}(\varphi) \subseteq U\}$. We may unwind this assertion as follows:

> For every open neighborhood U of e, and for every trio of functions $f_1, f_2, f_3 \in \mathscr{C}_c^+$ and every $\varepsilon > 0$, there exists a function $\varphi \in \mathscr{C}_c^+$ with $\text{supp}(\varphi) \subseteq U$ such that $|I(f_j) - I_\varphi(f_j)| < \varepsilon, j = 1,2,3$.

(This statement extends to any finite collection of f_j, but we shall need only three.) So given $f \in \mathscr{C}_c^+$ and $c \in \mathbf{R}$, we may simultaneously make $I(cf)$ arbitrarily close to $I_\varphi(cf)$ and $cI(f)$ arbitrarily close to $cI_\varphi(f)$. Appealing to Lemma 1-9 above, this shows that $I(cf) = cI(f)$. Similarly we have that I is left translation-invariant and at least subadditive. To see that I is in fact additive, we use Lemma 1-10 to choose a neighborhood U of e such that

$$I_\varphi(f_1) + I_\varphi(f_2) \le I_\varphi(f_1 + f_2) + \frac{\varepsilon}{4}$$

whenever $\text{supp}(\varphi) \subseteq U$. Then choose φ with $\text{supp}(\varphi) \subseteq U$ such that $I(f_1)$, $I(f_2)$, and $I(f_1 + f_2)$ all likewise lie within $\varepsilon/4$ of $I_\varphi(f_1)$, $I_\varphi(f_2)$, and $I_\varphi(f_1 + f_2)$, respectively. Since ε is arbitrary, it follows at once from the inequality above and the general sublinearity of I_φ that $I(f_1 + f_2) = I(f_1) + I(f_2)$, as required.

Finally, extend I to a positive left translation-invariant linear functional on $\mathscr{C}_c(G)$ by setting $I(f) = I(f^+) - I(f^-)$. As we remarked above, in view of our general discussion of translation-invariant measures and the Riesz representation theorem, this implies that G admits a left Haar measure μ and completes the existence proof. ❑

Uniqueness of Haar Measure

We now prove that the Haar measure on a locally compact group G is unique up to a positive scalar multiple. Given two Haar measures μ and ν on G, clearly it suffices to show that the ratio of integrals

$$\frac{\int_G f(x)\,d\mu}{\int_G f(x)\,d\nu}$$

is independent of $f \in \mathscr{C}_c^+$. To simplify the notation, we shall often write $I(f)$ and $J(f)$ for the indicated integrals with respect to μ and ν, respectively. Given two functions $f, g \in \mathscr{C}_c^+$, the plan is to produce a function $h \in \mathscr{C}_c^+$ such that the ratios $I(f)/J(f)$ and $I(g)/J(g)$ can both be made arbitrarily close to $I(h)/J(h)$.

Let K be a compact subset of G, the interior of which contains e. Then K contains an open symmetric neighborhood of the identity whose closure K_0 is compact and symmetric. (The symmetry is clearly preserved by closure.) Define compact subsets K_f and K_g of G by

$$K_f = \text{supp}(f) \cdot K_0 \cup K_0 \cdot \text{supp}(f) \quad \text{and} \quad K_g = \text{supp}(g) \cdot K_0 \cup K_0 \cdot \text{supp}(g) .$$

(Recall that the group product of compact sets is compact.) For $t \in K_0$, define $\gamma_t f$ by

$$\gamma_t f(s) = f(st) - f(ts) .$$

Equivalently, we have

$$\gamma_t f = R_t f - L_{t^{-1}} f .$$

Define $\gamma_t g$ similarly. Clearly $\gamma_t f$ and $\gamma_t g$ are supported in K_f and K_g, respectively, and both vanish on the center of G and in particular at e. Let $\varepsilon > 0$ be given. Then by left and right uniform continuity, K_0 contains an open neighborhood U_0 of e such that for all $s \in G$ and $t \in U_0$, both $|\gamma_t f(s)|$ and $|\gamma_t g(s)|$ are bounded by $\varepsilon/2$. Now U_0 in turn contains a symmetric open neighborhood U_1 of e whose closure K_1 is symmetric, compact, and contained in K_0. Moreover, by continuity we have that $|\gamma_t f(s)| < \varepsilon$ and $|\gamma_t g(s)| < \varepsilon$ for all $s \in G$ and all $t \in K_1$. The point is that as long as t remains in K_1, translation of f and g by t on either side has approximately the same effect.

We now construct h. We claim first that since e lies in the interior of K_1, there exists a second compact neighborhood K_2 of e such that K_2 is contained in the interior of K_1. Granting this, it follows immediately from Urysohn's lemma for locally compact topological spaces that there exists a continuous function $\tilde{h} : G \to \mathbf{R}_+$ that is 1 on K_2 and 0 outside of K_1. Define $h : G \to \mathbf{R}_+$ by

$$h(s) = \tilde{h}(s) + \tilde{h}(s^{-1}) .$$

Then certainly $h \in \mathscr{C}_c^+$, $\text{supp}(h)$ lies in K_1, and h is an even function in the sense that $h(s) = h(s^{-1})$.

PROOF OF CLAIM. Since G is Hausdorff and the boundary B of K_1 is likewise compact, B admits a finite cover by open sets each of which is disjoint from a corresponding open neighborhood of e in K_1. The intersection of these neighborhoods thus constitutes an open neighborhood U_2 of e in K_1, and we now set K_2 equal to the closure of U_2. Then by construction K_2 is contained in the interior of K_1, as required. ❑

We come to the main calculations. All integrals are implicitly over G and are translation-invariant, since μ and ν are by assumption Haar measures. First,

$$\begin{aligned} I(f)J(h) &= \iint f(s)h(t)d\mu_s d\nu_t \\ &= \iint f(ts)h(t)d\mu_s d\nu_t \ . \end{aligned}$$

The second calculation uses the property that h is even.

$$\begin{aligned} I(h)J(f) &= \iint h(s)f(t)d\mu_s d\nu_t \\ &= \iint h(t^{-1}s)f(t)d\mu_s d\nu_t \\ &= \iint h(s^{-1}t)f(t)d\mu_s d\nu_t \\ &= \iint h(t)f(st)d\mu_s d\nu_t \ . \end{aligned}$$

From these we can easily estimate the difference:

$$\begin{aligned} |I(h)J(f)-I(f)J(h)| &= |\iint h(t)\{f(st)-f(ts)\}\,d\mu_s d\nu_t\,| \\ &= |\iint h(t)\gamma_t f(s)\,d\mu_s d\nu_t\,| \\ &\leq \varepsilon\mu(K_f)J(h) \ . \end{aligned}$$

The point in the last line of the calculation is that supp(h) lies in a K_1 where $\gamma_t f$ is small. Similarly,

$$\begin{aligned} |I(h)J(g)-I(g)J(h)| &= |\iint h(t)\{g(st)-g(ts)\}\,d\mu_s d\nu_t| \\ &= |\iint h(t)\gamma_t g(s)\,d\mu_s d\nu_t| \\ &\leq \varepsilon\mu(K_g)J(h) \ . \end{aligned}$$

Dividing the first inequality by $J(h)J(f)$ yields

$$\left|\frac{I(h)}{J(h)}-\frac{I(f)}{J(f)}\right| \leq \frac{\varepsilon\mu(K_f)}{J(f)} \ .$$

Dividing the second by $J(h)J(g)$ yields

$$\left|\frac{I(h)}{J(h)}-\frac{I(g)}{J(g)}\right| \leq \frac{\varepsilon\mu(K_g)}{J(g)} \ .$$

Since ε is arbitrary, this shows that the ratio $I(f)/J(f)$ is independent of f as claimed. ❑

1.3 Profinite Groups

This section introduces a special class of topological groups of utmost importance to our subsequent work. We begin by establishing a categorical framework for the key definition that follows.

Projective Systems and Projective Limits

Let I be a nonempty set, which shall later serve as a set of indices. We say that I is *preordered* with respect to the relation $\leq$ if the given relation is reflexive (i.e., $i \leq i$ for all $i \in I$) and transitive (i.e., $i \leq j$ and $j \leq k \Rightarrow i \leq k$ for all $i, j, k \in I$). Note that we do not assume antisymmetry (i.e., $i \leq j$ and $j \leq i$ need not imply that $i = j$); hence a preordering is weaker than a partial ordering. Clearly the elements of a preordered set I constitute the objects of a category for which there is a unique morphism connecting two elements i and j if and only if $i \leq j$.

We say that a preordered set I is moreover a *directed set* if every finite subset of I has an upper bound in I; equivalently, for all $i, j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$. (Recall that directed sets are precisely what is needed to define the notion of a net in an abstract topological space.) While most of the specific instances of preordered sets that we meet below will moreover be directed, we shall need only the preordering for the general categorical constructions to follow. Beware, however, that directed sets will play a crucial but subtle role in establishing that the projective limit of nonempty sets is itself nonempty. (See Proposition 1-11.)

Example. The integers **Z** are preordered (but not partially ordered) with respect to divisibility and in fact constitute a directed set: a finite collection of integers is bounded with respect to divisibility by its least common multiple.

Assume that I is a preordered set of indices and let $\{G_i\}_{i \in I}$ be a family of sets. Assume further that for every pair of indices $i, j \in I$ with $i \leq j$ we have an associated mapping $\varphi_{ij}: G_j \to G_i$, subject to the following conditions:

(i) $\varphi_{ii} = 1_{G_i} \quad \forall i \in I$

(ii) $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik} \quad \forall i, j, k \in I, i \leq j \leq k$

Then the system (G_i, φ_{ij}) is called a *projective* (or *inverse*) *system*. Note that if we regard I as a category, then the association $i \mapsto G_i$ defines a contravariant functor.

DEFINITION. Let (G_i, φ_{ij}) be a projective system of sets. Then we define the *projective limit* (or *inverse limit*) of the system, denoted $\underset{\leftarrow}{\lim} G_i$, by

$$\underset{\leftarrow}{\lim} G_i = \{(g_i) \in \prod_{i \in I} G_i : i \leq j \Rightarrow \varphi_{ij}(g_j) = g_i \} .$$

Note that as a subset of the direct product, $\underset{\leftarrow}{\lim} G_i$ comes naturally equipped with a family of projection maps $p_j : \underset{\leftarrow}{\lim} G_i \to G_j$, and with regard to these projections, the projective limit manifests the following universal property:

UNIVERSAL PROPERTY. *Let H be a nonempty set and let there be given a system of maps $(\psi_i : H \to G_i)_{i \in I}$ that is compatible with the projective system (G_i, φ_{ij}) in the sense that for each pair of indices $i, j \in I$ with $i \leq j$, the following diagram commutes:*

$$\begin{tikzcd}
 & H \arrow[dl, "\psi_j"'] \arrow[dr, "\psi_i"] & \\
G_j \arrow[rr, "\varphi_{ij}"'] & & G_i
\end{tikzcd}$$

Then there exists a unique map $\psi : H \to \underset{\leftarrow}{\lim} G_i$ such that for each $i \in I$ the diagram

$$\begin{tikzcd}
H \arrow[r, "\psi"] \arrow[dr, "\psi_i"'] & \underset{\leftarrow}{\lim} G_i \arrow[d, "p_i"] \\
 & G_i
\end{tikzcd}$$

also commutes.

The mapping ψ is of course none other than $h \mapsto (\psi_i(h))_{i \in I}$, just as for the direct product of sets, but in this case the compatibility of the ψ_i guarantees that the image falls into the projective limit.

Note carefully that neither the definition of a projective limit nor the associated universal property asserts that a given projective limit of sets is nonempty. In particular, the projection maps may have empty domain. Of course, if a compatible system $(\psi_i : H \to G_i)_{i \in I}$ exists with nonempty domain H, then one infers from the existence of elements of the form $(\psi_i(h))_{i \in I}$ that the projective limit is likewise nonempty.

The construction of the projective limit works equally well in the category of groups (in which case the set maps are replaced by group homomorphisms, and the group operation is defined componentwise) or the category of topological spaces (in which case the set maps must be replaced by continuous functions, and the topology on the projective limit is the subspace product topology induced from the direct product). In the case of groups, note that the projective limit is never empty, since the identity element of the direct product clearly lies in the projective limit. It follows from these remarks that the projective limit of a projective system of topological groups is itself a topological group with respect to the componentwise multiplication and the subspace topology.

REMARK. A more obvious topology on a product space $\prod X_i$ is the *box topology*, generated by sets of the form $\prod U_i$ with U_i open in X_i for all i. But this is a much finer topology than the standard product topology. Moreover, with respect to the box topology the product of compact spaces need not be compact.

In the following subsection we shall be concerned with projective limits of finite groups. In passing we shall require conditions under which the projective limit of finite sets is nonempty. It is here that the notion of a directed set reappears critically.

1-11 PROPOSITION. *Assume that I is a directed set, and let (G_i, φ_{ij}) be a projective system of finite sets. Set $G = \underset{\leftarrow}{\lim} G_i$. Then:*

(i) *If each G_i is nonempty, G is nonempty.*

(ii) *For each index $i \in I$,*

$$p_i(G) = \bigcap_{i \leq j} \varphi_{ij}(G_j) \ .$$

PROOF. Our proof is adapted from a more general result in Bourbaki's *Theory of Sets*, Chapter III, § 7.4. Let us call $(S_i)_{i \in I}$ a *compatible family* (with respect to our given projective system) if the following conditions are satisfied:

(a) For all $i \in I$, $S_i \subseteq G_i$.

(b) For all $i, j \in I$ with $i \leq j$, $\varphi_{ij}(S_j) \subseteq S_i$.

(c) For all $i \in I$, $S_i \neq \emptyset$.

Note well that if (S_i) is a compatible family of the form $S_i = \{x_i\}$ for all $i \in I$, then in fact $(x_i) \in G$, which in this case is *ipso facto* nonempty.

Henceforth let Σ denote the set of all compatible families. We impose an ordering on Σ as follows: given compatible families (S_i) and (T_i), we shall write $(S_i) \leq (T_i)$ if $S_i \supseteq T_i$ for all i. If Σ' is a totally ordered subset of Σ, then clearly Σ' admits the upper bound (T_i) defined by

$$T_i = \bigcap_{(S_j)\in\Sigma'} S_i \ .$$

Conditions (a)–(c) are trivially satisfied, and only the last of these requires finiteness. Hence the given ordering is inductive.

Suppose that there exists a maximal compatible system $(S_i)\in\Sigma$. We claim that $S_i=\varphi_{ij}(S_j)$ for all $i\leq j$. To prove this, let (T_i) be defined by

$$T_i = \bigcap_{i\leq j} \varphi_{ij}(S_j) \subseteq S_i \ .$$

Since (S_i) is assumed maximal, our claim is established, provided that we can show that also $(T_i)\in\Sigma$. Again (a) and (b) are routine; (c) is interesting. First observe that if $i\leq j\leq k$, then $\varphi_{ik}(S_k)\subseteq\varphi_{ij}(S_j)$. Now consider the intersection that defines T_i. Each of the factors appearing is a subset of the finite set S_i. There are only finitely many such subsets, and consequently we may assume that the intersection is over a finite set of indices $j_1,\dots,j_r$. *But I is directed, so there exists an element k in I such that* $k\geq j_1,\dots,j_r$. Thus by our previous observation,

$$\varphi_{ik}(S_k) \subseteq \bigcap_{m=1}^{r} \varphi_{ij_m}(S_{j_m}) = T_i$$

and therefore T_i is manifestly nonempty.

We continue to assume that (S_i) is maximal in Σ and shall demonstrate next that each S_i contains exactly one element. Fix i and let $x_i\in S_i$. Define (T_j) as follows:

$$T_j = \begin{cases} S_j \cap \varphi_{ij}^{-1}(x_i) & \text{if } i\leq j \\ S_j & \text{otherwise.} \end{cases}$$

Note in particular that $T_i=\{x_i\}$, since φ_{ii} is the identity on S_i. Then (T_j) lies in Σ: (a) is obvious, (b) is an easy exercise, and (c) follows from the claim of the previous paragraph, namely that $S_i=\varphi_{ij}(S_j)$ for all $j\geq i$. Moreover, by construction $(S_j)\leq(T_j)$, whence, since (S_j) is maximal, we must in fact have equality. This shows that $S_i=\{x_i\}$. Since i was arbitrary, this suffices.

We now address both statements of the proposition. Again fix $i\in I$. By definition of a projective system,

$$p_i(G) \subseteq \bigcap_{i\leq j} \varphi_{ij}(G_j) \ .$$

One may argue as above that since all but finitely many factors on the right are redundant, the given intersection is nonempty; thus it contains an element x_i. Define (T_j) as follows:

$$T_j = \begin{cases} \varphi_{ij}^{-1}(x_i) & \text{if } i\leq j \\ G_j & \text{otherwise.} \end{cases}$$

Note in particular that $T_i=\{x_i\}$. One sees without difficulty that $(T_j)\in\Sigma$ (at last establishing that Σ is nonempty!), and so by Zorn's lemma there is a maximal element (S_j) of Σ with the additional property that $(S_j)\geq(T_j)$. But then $(S_j)=\{y_j\}$ and G is nonempty, as required by (i). Moreover, $x_i=y_i\in p_i(G)$, which in light of the preceding inclusion establishes (ii). □

Profinite Groups

We now come to the principal definition of this section. It may seem at first to be essentially group-theoretic, with the topology as an afterthought, but we shall see shortly that this is not the case.

Consider a projective system of finite groups, each of which we take as having the discrete topology. Their projective limit acquires the relative topology induced by the product topology on the full direct product. This is called the *profinite topology*, and accordingly the projective limit acquires the structure of a topological group.

DEFINITION. A topological group isomorphic to the projective limit of a projective system of finite groups (endowed with the profinite topology) is called a *profinite group*.

The following proposition summarizes the most fundamental global properties of a profinite group.

1-12 PROPOSITION. *Let G be a profinite group, given as the projective limit of the projective system* (G_i,φ_{ij}). *Then the following assertions hold:*

(i) *G is Hausdorff with respect to the profinite topology.*

(ii) *G is a closed subset of the direct product* $\prod G_i$.

(iii) *G is compact.*

PROOF. (i) The direct product of Hausdorff spaces is also Hausdorff, and any subset of a Hausdorff space is clearly also Hausdorff in the induced topology.

(ii) We may realize the complement of G in $\prod G_i$ as an open set as follows:

$$G^c = \bigcup_i \bigcup_{j\geq i} \{(g_k) \in \prod G_k : \varphi_{ij}(g_j) \neq g_i\} \ .$$

Therefore G is closed, as claimed.

(iii) Since the direct product $\prod G_i$ is compact by Tychonoff's theorem, this assertion follows from (ii) on general principles: a closed subset of a compact space is itself compact. □

EXAMPLES

(1) Let $G_n = \mathbf{Z}/n\mathbf{Z}$, $n \geq 1$, the additive group of integers modulo n. Then $\{G_n\}$ is a projective system, since there is a canonical projection

$$\begin{aligned} \varphi_{mn} : \mathbf{Z}/n\mathbf{Z} &\to \mathbf{Z}/m\mathbf{Z} \\ [k]_n &\mapsto [k]_m \end{aligned}$$

whenever $m|n$, and these projections are clearly compatible in the required sense. We may thus form their projective limit

$$\hat{\mathbf{Z}} = \varprojlim \mathbf{Z}/n\mathbf{Z} \ .$$

Note that $\hat{\mathbf{Z}}$ also admits the structure of a topological ring.

(2) Let $H_n = (\mathbf{Z}/n\mathbf{Z})^\times$, $n \geq 1$, the group of units in $\mathbf{Z}/n\mathbf{Z}$. Then $\{H_n\}$ is a projective system, since a (unital) ring homomorphism maps units to units. Set

$$\hat{\mathbf{Z}}^\times = \varprojlim (\mathbf{Z}/n\mathbf{Z})^\times \ .$$

Then $\hat{\mathbf{Z}}^\times$ is a topological group under multiplication and in fact is the group of units of $\hat{\mathbf{Z}}$.

(3) Fix a rational prime p and set $G_m = \mathbf{Z}/p^m\mathbf{Z}$, $m \geq 1$. Again $\{G_m\}$ is a projective system, and we form its projective limit to obtain a ring

$$\mathbf{Z}_p = \varprojlim \mathbf{Z}/p^m\mathbf{Z} \ .$$

This is called *the ring of p-adic integers.*

(4) Let $H_m = (\mathbf{Z}/p^m\mathbf{Z})^\times$, $m \geq 1$, so that $\{H_m\}$ is a projective system as in Example 2. Then set

$$\mathbf{Z}_p^\times = \varprojlim (\mathbf{Z}/p^m\mathbf{Z})^\times \ .$$

One checks easily that $\mathbf{Z}_p^\times$ is the group of units in $\mathbf{Z}_p$; this is called *the group of p-adic units.*

(5) The set of all finite Galois extensions $K/\mathbf{Q}$ within a fixed algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ forms a directed set with respect to inclusion. We have a corresponding directed system of finite groups $\mathrm{Gal}(K/\mathbf{Q})$, where if $K \subseteq L$, the associated homomorphism $\mathrm{Gal}(L/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q})$ is just restriction. Moreover, we have an isomorphism

$$\begin{aligned} \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) &\xrightarrow{\approx} \varprojlim \mathrm{Gal}(K/\mathbf{Q}) \\ \sigma &\mapsto (\sigma|_K) \ . \end{aligned}$$

Topological Characterization of Profinite Groups

Recall that a topological space X is called *connected* if whenever $X = U \cup V$ for nonempty open subsets U and V, then $U \cap V \neq \varnothing$. (Evidently an equivalent statement results if we substitute nonempty closed subsets for open ones.) Every point $x \in X$ is contained in a maximal connected subset of X, which is called the *connected component* of x. In the special case of a topological group G, the connected component of the identity e is denoted G°.

A topological space X is called *totally disconnected* if every point in X is its own connected component. Clearly a homogeneous space is totally disconnected if and only if some point is its own connected component. In particular, a topological group G is totally disconnected if and only if $G^\circ = \{e\}$.

1-13 LEMMA. *G° is a normal subgroup of G. Moreover, the quotient space G/G° is totally disconnected, whence $(G/G^\circ)^\circ$ is the trivial subgroup of the quotient.*

PROOF. Let $x \in G^\circ$. Then $x^{-1}G^\circ$ is connected (by homogeneity) and contains e, whence $x^{-1}G^\circ \subseteq G^\circ$. Thus G° is closed under inverses. The same argument now shows that $xG^\circ \subseteq G^\circ$, and that for all $y \in G$, we have further that $yG^\circ y^{-1} \subseteq G^\circ$. Consequently G° is indeed a normal subgroup of G°, as claimed. The second statement is immediate: by homogeneity, the connected components of G are precisely the elements of G/G°, and so by general topology (see Exercise 5 below), G/G° is totally disconnected. □

1-14 THEOREM. *Let G be a topological group. Then G is profinite if and only if G is compact and totally disconnected.*

PROOF. ⇒) We have already seen that G is compact. Thus it remains to show that $G^\circ=\{e\}$. Let U be any open subgroup of G. Then $U\cap G^\circ$ is open in G° and nonempty. Now consider the subset V of G defined by

$$V = \dot{\bigcup_{x\in G^\circ - U}} x\cdot(U\cap G^\circ) .$$

Then since each $x\cdot(U\cap G^\circ)$ is open in G°, so is V. Moreover, by elementary group theory, $U\cap V=\varnothing$, and G° is the disjoint union of two open sets, namely $U\cap G^\circ$ and V. But by definition G° is connected, so either $U\cap G^\circ$ or V must be empty. Since the former is not, the latter is, and in fact $G^\circ=U\cap G^\circ$, which is to say that $G^\circ\subseteq U$. Since U is an arbitrary open subgroup of G, we have accordingly,

$$G^\circ\subseteq \bigcap_{\substack{U \text{ an open} \\ \text{subgroup of } G}} U .$$

We must now make use of the profinite nature of G. Indeed, let

$$G=\lim_{\leftarrow} G_i$$

where each G_i is a finite group with the discrete topology. Recall that for each index i we have a projection map $p_i : G\to G_i$ that is just the restriction of the corresponding map on the full direct product. Let $y=(y_i)$ lie in G and assume that y is not the identity element. Then for some index i_0, it must be the case that $y_{i_0}\neq e_{i_0}$. But now consider the set $U_0=p_{i_0}^{-1}(e_{i_0})$. Since the topology on G_{i_0} is discrete and the projections are continuous, U_0 is open in G. Since the projections are moreover group homomorphisms, U_0 is in fact a subgroup of G. But by construction, U_0 excludes y. This shows that the only element in the intersection of all open subgroups of G is the identity. Thus G° is trivial, as required.

The proof of the converse is more delicate and requires three lemmas. We begin with some preliminary analysis.

Let $\mathscr{N}$ be the family of open, normal subgroups of G. This is clearly a directed set with respect to the relation $M\leq N$ if $N\subseteq M$. (In fact, two subgroups M and N in $\mathscr{N}$ have a least upper bound $M\cap N$ in $\mathscr{N}$.) Moreover, the following observations are elementary:

(i) For each $N\in\mathscr{N}$, the quotient group G/N is both compact and discrete, hence finite.

(ii) For each pair of subgroups $M,N\in\mathscr{N}$, with $M\leq N$, the kernel of the canonical projection $G\to G/M$ contains N, and hence this map factors through G/N to yield the induced map

$$\begin{aligned} \varphi_{M,N} : G/N &\to G/M \\ xN &\mapsto xM . \end{aligned}$$

From this description it is clear that if $L\leq M\leq N$ in $\mathscr{N}$, then

$$\varphi_{L,M}\circ\varphi_{M,N}=\varphi_{L,N}$$

and $\{G/N\}_{N\in\mathscr{N}}$ constitutes a projective system of finite groups.

The point, of course, is to show that G is isomorphic to the projective limit of this system.

1-15 LEMMA. *Let the profinite group G' be given by*

$$G'=\lim_{\substack{\leftarrow \\ N}} G/N$$

where N varies over $\mathscr{N}$, as defined above. Then there exists a surjective, continuous homomorphism α: $G\to G'$.

PROOF. For $N\in\mathscr{N}$ let α_N denote the canonical projection from G to G/N, which is surjective. Since G/N is homogeneous, we establish that α_N is also continuous by noting that $\alpha_N^{-1}(e_{G/N})=N$, which by hypothesis is open in G. Arguing as in (ii) above, it is clear that whenever $M\leq N$ in $\mathscr{N}$, the following triangle is commutative:

$$\begin{tikzcd} & G/N \arrow[dd, "\varphi_{M,N}"] \\ G \arrow[ur, "\alpha_N"] \arrow[dr, "\alpha_M"'] & \\ & G/M \end{tikzcd}$$

Thus by the universal property of projective limits, we have a continuous homomorphism $\alpha : G\to G'$ such that $\alpha_N=p_N\circ\alpha$ for all $N\in\mathscr{N}$, where p_N denotes projection from G' onto G/N, the component of the projective limit corresponding to N.

It remains to show that α is surjective. We claim that α has dense image in G'. Granting this, we conclude the argument as follows: Since G is compact and G' is Hausdorff, the image of α is, moreover, closed in G'. Thus $\mathrm{Im}(\alpha)$, being dense, must be all of G', as required.

To establish the claim we shall show that no open subset of G' is disjoint from $\mathrm{Im}(\alpha)$. Consider the topology of G': this is generated by sets of the form $p_N^{-1}(S_N)$, where S_N is an arbitrary subset of G/N. Every open set in G' is thus expressible as a union of finite intersections of these $p_N^{-1}(S_N)$. Such an intersection U consists of elements of the form

$$(\bar{x}_N)_{N\in\mathcal{N}}$$

where at most only finitely many of the coordinates are constrained to lie in some given proper subset of the corresponding quotient; the rest are unrestricted. Now suppose that the constrained coordinates correspond to the subgroups $N_1,\ldots,N_r$ and that

$$M=\bigcap_{j=1}^{r} N_j \ .$$

Then given $(x_N)\in G'$, the coordinates x_{N_j} are all determined as images of the coordinate x_M under the associated projection maps. Since $\alpha_M\colon G\to G/M$ is surjective, there is at least one element in $t\in G$ such that $\alpha(t)_M=x_M$, and consequently t also satisfies $\alpha(t)_{N_j}=x_{N_j}$ for $j=1,\ldots,r$. In particular, if $(x_N)\in U$, then certainly $\alpha(t)\in U$, since $\alpha(t)$ agrees with (x_N) in all of the constrained coordinates. Thus U manifestly intersects $\mathrm{Im}(\alpha)$, and by our previous remarks, so, too, does every open set in G'. This completes the proof. □

1-16 LEMMA. *Let X be a compact Hausdorff space. For a fixed point $P\in X$, set $\mathscr{U}=\{K\colon K$ is a compact, open neighborhood of $P\}$. Define $Y\subseteq X$ by*

$$Y=\bigcap_{K\in\mathscr{U}} K \ .$$

Then Y is connected.

PROOF. Note that the collection $\mathscr{U}$ is nonempty because X itself is compact and open.

Suppose that Y is the disjoint union of closed subsets Y_1 and Y_2. We must show that either Y_1 or Y_2 is empty. Recall from general topology that a compact Hausdorff space is normal. Accordingly, there exist disjoint open subsets U_1 and U_2 containing, respectively, Y_1 and Y_2. Now set $Z=X-(U_1\cup U_2)$, which is closed and therefore compact. Since $Y\subseteq U_1\cup U_2$, Z and Y are disjoint, which is to say that Z lies in the complement of Y. Thus we have an open cover for Z

$$Z\subseteq\bigcup_{K\in\mathscr{U}} K^c$$

that admits a finite subcover. Hence there exist $K_1,\ldots,K_r\in\mathscr{U}$ such that

$$Z\cap(\bigcap_j K_j)=\varnothing \ .$$

Let W denote the intersection of the K_j. Then W is a compact, open neighborhood of P, and so W is itself in $\mathscr{U}$. But also

$$W=(W\cap U_1)\ \dot\cup\ (W\cap U_2)$$

since W is disjoint from Z, the complement of $U_1\cup U_2$. We now make note of the following assertions:

(i) Both $W\cap U_1$ and $W\cap U_2$ are compact, open subsets of X.

(ii) P lies exclusively in one of $W\cap U_1$ or $W\cap U_2$. Say $P\in W\cap U_1$.

From (i) and (ii) it follows that $W\cap U_1\in\mathscr{U}$ and so $Y\subseteq W\cap U_1$. Since $Y_2\subseteq Y$ and Y_2 is disjoint from U_1, it follows that Y_2 is empty, as required. □

1-17 LEMMA. *Let G be a compact, totally disconnected topological group. Then every neighborhood of the identity contains an open normal subgroup.*

PROOF. As a preliminary, note that G is Hausdorff: If x and y are distinct points in G, then $\{x,y\}$ is disconnected with respect to the subspace topology. Therefore there exist respective open neighborhoods of x and y that are disjoint. The proof now proceeds in three steps: First, we show that every open neighborhood U of the identity contains a compact, open neighborhood W of the identity. Second, we show that W in turn contains an open, symmetric neighborhood V of the identity such that $WV\subseteq W$. Third, from V we construct an open subgroup, then an open, normal subgroup of G contained in U, as required.

Let $\mathscr{U}$ denote the set of all compact, open neighborhoods of the group identity e. Applying the previous lemma with $P=e$, we find that

$$Y=\bigcap_{K\in\mathscr{U}} K$$

is a connected set containing e. But G is totally disconnected, so in fact $Y=\{e\}$. Now let U denote any open neighborhood of e. Then $G-U$ is closed and therefore compact. Since e is the only element of G common to all of the K in

$\mathscr{U}$, there exist subsets $K_1,\dots,K_r\in\mathscr{U}$ whose complements cover $G-U$, and therefore

$$W=\bigcap_{j=1}^{r}K_j$$

is a subset of U and a compact, open neighborhood of e. In particular, $W\in\mathscr{U}$. This completes the first step.

To begin the second step, consider the continuous map $\mu\colon W\times W\rightarrow G$ defined by restriction of the group operation. We make the following observations:

(i) For every $w\in W$, the point $(w,e)\in\mu^{-1}(W)$.

(ii) Since W is open, the inverse image of W itself under μ is open in $W\times W$.

(iii) It follows from (i) and (ii) that for every $w\in W$, there exists open neighborhoods U_w of w and V_w of e such that $U_w\times V_w\subseteq\mu^{-1}(W)$. Moreover, by Proposition 1-1, we may assume that each V_w is symmetric.

(iv) The collection of subsets U_w $(w\in W)$ constitutes an open cover for W. Since W is compact, a finite subcollection $U_1,\dots,U_r$ suffices.

Let $V_1,\dots,V_r$ correspond to $U_1,\dots,U_r$ in (iii) above. Define an open neighborhood $V\subseteq W$ of the identity as follows:

$$V=\bigcap_{j=1}^{r}V_j\ .$$

By construction $WV\subseteq W$, and by induction $WV^n\subseteq W$ for all $n\geq0$. In particular, $V^n\subseteq W$ for all $n\geq0$. This completes the second step.

For the final step, we expand V to an open subgroup O of G contained in W by the formula

$$O=\bigcup_{n=1}^{\infty}V^n\ .$$

(Note that O is closed under inversion because V is symmetric.) The quotient space G/O is compact and discrete, hence finite, so we can find a finite collection of coset representatives $x_1,\dots,x_s$ for O in G. It follows that O likewise has only finitely many conjugates in G: all take the form

$$x_jOx_j^{-1}\qquad(j=1,\dots,s)\ .$$

Thus

$$N=\bigcap_{j=1}^{s}x_jOx_j^{-1}$$

is an open, normal subgroup of G. Moreover, since one of the conjugates of O is O itself, $N\subseteq O\subseteq W\subseteq U$. This completes the proof. □

This brings us at last to the conclusion of the topological characterization of profinite groups.

Proof of Theorem 1-14, Converse. By Lemma 1-15, we have a surjective homomorphism $\alpha\colon G\rightarrow G'$, where G' is the projective limit of the finite quotients G/N for N an open, normal subgroup of G (i.e., $N\in\mathscr{N}$). Appealing to Exercise 9 below, we see that it suffices to show that α has trivial kernel and hence is injective.

Since α simultaneously projects on all of the quotients, it is clear that

$$\mathrm{Ker}(\alpha)=\bigcap_{N\in\mathscr{N}}N\ .$$

By the previous lemma, every open neighborhood of $e\in G$ contains an open, normal subgroup, which is therefore represented in the intersection above. It follows that Ker(α) is contained in *every* neighborhood of e and hence in the intersection of all such neighborhoods. But G is Hausdorff: the intersection of all neighborhoods of e consists merely of e itself. Hence Ker(α) is indeed trivial, and the theorem is proved. □

The Structure of Profinite Groups

The following theorem shows in particular that closed subgroups of profinite groups and profinite quotients by closed normal subgroups are likewise profinite.

1-18 Theorem. *Let G be a profinite group and let H be a subgroup of G. Then H is open if and only if G/H is finite, Moreover, the following three statements are equivalent.*

? and discrete?

(i) *H is closed.*

(ii) *H is profinite.*

(iii) *H is the intersection of a family of open subgroups.*

Finally, if (i)–(iii) *are satisfied, then G/H is compact and totally disconnected.*

PROOF. The first statement follows from Proposition 1-4, part (iv), since a profinite group is necessarily compact. We next establish the given equivalences.

(i)⇒(ii) H is a closed subset of a compact space and therefore itself compact. Hence it remains to show that H is totally disconnected. But this is trivial: since $G^\circ=\{e\}$, also $H^\circ=\{e\}$, and this suffices by homogeneity.

(ii)⇒(i) If H is itself profinite, it is a compact subset of a Hausdorff space and hence closed.

(iii)⇒(i) Suppose that H is the intersection of some family of open subgroups of G. Then since every open subgroup is also closed [Proposition 1-1, part (iv)], H is also the intersection of a family of closed subgroups of G, and therefore itself closed.

(i)⇒(iii) As above, let $\mathscr{N}$ denote the family of all open, normal subgroups of G. If $N\in\mathscr{N}$, then since N is normal, NH is a subgroup of G. By part (i), $[G:N]$ is finite, whence $[G:NH]$ is likewise finite and NH is open. Moreover, clearly

[illegible] Nh; $h\in H$

$$H\subseteq\bigcap_{N\in\mathscr{N}}NH\ .$$

It remains only to demonstrate the opposite inclusion. So let x lie in the indicated intersection, and let U be any neighborhood of x. Then Ux^{-1} is a neighborhood of e, and so by Lemma 1-16, Ux^{-1} contains some $N_0\in\mathscr{N}$. Since x lies in the given intersection, $x\in N_0H$. Now by construction, also $x\in N_0x$. Hence N_0x is equal to N_0h for some $h\in H$, and consequently $h\in N_0x\subseteq U$. The upshot is that every neighborhood of x intersects H, and hence x lies in the closure of H. But H is closed by hypothesis, and therefore $x\in H$, as required. 1-17

For the final statement, the compactness of the quotient follows at once from the compactness of G. Let $\rho:G\to G/H$ denote the canonical map. To see that G/H is totally disconnected, assume that $\rho(X)$ is a connected subset of G/H that properly contains $\rho(H)$. Then $Y=X-H$ is nonempty, and since we may assume that H is nontrivial, Y contains more than one point. Hence Y is the disjoint union of nonempty open (hence closed) sets F_1 and F_2. One checks easily that since H is closed, F_1 and F_2 are both open (hence closed) in X. Thus X is the disjoint union of the two nonempty closed sets $F_1\cup H$ and F_2. But then the image of F_2 under ρ is (a) nonempty, (b) not the full image of X, and (c) both open and closed in $\rho(X)$. Since $\rho(X)$ is connected, this is a contradiction. Hence the connected component of $\rho(H)$ is $\rho(H)$ itself, and the quotient is totally disconnected, as claimed. □

X [illegible] $X=\rho^{-1}(\rho X)$?

A Little Galois Theory

We close this section by showing how profinite groups make a momentous appearance in connection with the Galois theory of infinite extensions. To begin, we recall the following elements of field theory:

(i) Let F be a field. An element a that is algebraic over F is called *separable* if the irreducible polynomial of a over F has no repeated roots. An algebraic field extension K/F is called *separable* if every element of K is separable over F.

(ii) Assume that K is an algebraic extension of F contained in an algebraic closure $\overline{F}$ of F. Then we call K/F a *normal* extension if every embedding of K into $\overline{F}$ that restricts to the identity on F is in fact an automorphism of K. (We say that such an automorphism is an automorphism of K *over* F.)

(iii) A field extension K/F is called a *Galois extension* if it is both separable & algebraic and normal. The set of all automorphisms of K over F constitutes a group under composition; this is called the *Galois group* of K over F and denoted Gal(K/F). If $F\subseteq L\subseteq K$ is a tower of fields and K/F is Galois, then K/L is likewise Galois.

Note that these notions do not require that K/F be finite. Our aim now is to extend the fundamental theorem of Galois theory to infinite extensions. This will require the introduction of some topology.

If S is any set of automorphisms of a field F, as usual F^S denotes the fixed field of S in F; that is, the subfield of F consisting of all elements of F left fixed by every automorphism of S.

Suppose that K/F is a Galois extension with Galois group G. Consider the set $\mathscr{N}$ of normal subgroups of G of finite index. If $N,M\in\mathscr{N}$ and $M\subseteq N$, we have a projection map $\rho_{N,M}:G/M\to G/N$, and hence a projective system of quotients $\{G/N\}_{N\in\mathscr{N}}$. This system is certainly compatible with the family of canonical projections $\rho_N:G\to G/N$, which corresponds to the restriction map from Gal(K/F) to Gal(K^N/F). Thus we have a canonically induced homomorphism ρ from G into the projective limit of the associated quotients.

1-19 PROPOSITION. *Let K, F, G, and $\mathscr{N}$ be as above. Then the canonical map*

$$\rho:G\to\varprojlim_{N\in\mathscr{N}}G/N$$

is in fact an isomorphism of groups. Hence G is a profinite group in the topology induced by ρ.

In this context, we shall simply speak of the Galois group G as having the profinite topology.

PROOF. We show first that ρ is injective. Certainly

$$\operatorname{Ker}(\rho) = \bigcap_{N \in \mathscr{N}} N$$

and so we need only demonstrate that this intersection is trivial. Let $\sigma \in \operatorname{Ker}(\rho)$ and let $x \in K$. Then by elementary field theory there exists a finite Galois extension F'/F such that $F' \subseteq K$ and $x \in F'$. Now the restriction map from $G = \operatorname{Gal}(K/F)$ to $\operatorname{Gal}(F'/F)$ has kernel $\operatorname{Gal}(K/F')$, which is therefore a normal subgroup of G of finite index. But then $\sigma \in \operatorname{Gal}(K/F')$, and so $\sigma(x) = x$. Since x is arbitrary, σ is the identity on K, and $\operatorname{Ker}(\rho)$ is trivial, as required.

[illegible]
[illegible] algebraic

We show next that ρ is also surjective. Fix (σ_N) in the projective limit. Given an arbitrary element $x \in K$, again we know that x lies in some finite Galois extension F' of F with $N = \operatorname{Gal}(K/F')$ normal and of finite index in G and $\operatorname{Gal}(F'/F) = G/N$. Now define $\sigma \in \operatorname{Gal}(K/F')$ by $\sigma(x) = \sigma_N(x)$. By construction of the projective limit, σ is independent of the choice of extension F', and hence is a well defined automorphism of K. Moreover, it is clear that σ_N is $\rho_N(\sigma)$ for all N. □

Note that the isomorphism constructed in the previous proposition is essentially field-theoretic, and not merely group-theoretic. (See Exercise 12 below.)

normal
separable
algebraic

1-20 THEOREM. (The Fundamental Theorem of Galois Theory) *Let K/F be a Galois extension (not necessarily finite) and let $G = \operatorname{Gal}(K/F)$ with the profinite topology. Then the maps*

$$\alpha : L \mapsto H = \operatorname{Gal}(K/L)$$

$$\beta : H \mapsto L = K^H$$

constitute a mutually inverse pair of order-reversing bijections between the set of intermediate fields L lying between K and F, and the set of closed subgroups of G. Moreover, L is Galois over F if and only if the corresponding subgroup H is normal in G.

PROOF. Note that in the case of a finite extension K/F, we may ignore the topological restriction, and the statement amounts to the fundamental theorem of Galois theory for finite extensions, a result that we assume. We proceed in four steps.

STEP 1. We must show first that the map α is well-defined; that is, that α indeed yields closed subgroups of G. (The map β is of course well-defined on arbitrary subsets of G.) According to the previous proposition, H is profinite as the Galois group of K/L, and Exercise 14 shows that this topology is identical to that induced by G. Thus H is a profinite subgroup of a profinite group and is therefore closed by Theorem 1-18.

STEP 2. We claim that $\beta \circ \alpha$ is the identity map. Let L be an intermediate field. By definition $\alpha(L)$ fixes L, and so clearly $\beta(\alpha(L)) \supseteq L$. Conversely, suppose that z lies in $\beta(\alpha(L))$. Then since z lies in K and is therefore separable over L, z also belongs to a finite Galois extension M of L contained in K. Let $\overline{\sigma} \in \operatorname{Gal}(M/L)$. Then there exists $\sigma \in \operatorname{Gal}(K/L)$ that restricts to $\overline{\sigma}$. (The extensibility of automorphisms for infinite extensions follows from the finite case by Zorn's lemma.) By construction, $\sigma(z) = z$, and hence $\overline{\sigma}(z) = z$ for all $\overline{\sigma} \in \operatorname{Gal}(M/L)$. But by the fundamental theorem for finite extensions, we know that $z \in L$. Hence we have also that $\beta(\alpha(L)) \subseteq L$, and the claim is established.

STEP 3. We shall show now that $\alpha \circ \beta$ is likewise the identity. By definition, for any subgroup H of G we have that $\alpha(\beta(H)) \supseteq H$. Now assume that H is closed. Then again by Theorem 1-18, H is the intersection of a family $\mathscr{U}$ of open subgroups of G. Since α and β are clearly order reversing,

$$\beta(H) = \beta\Big(\bigcap_{U \in \mathscr{U}} U\Big) \supseteq \bigcup_{U \in \mathscr{U}} \beta(U)$$

and

$$\alpha(\beta(H)) \subseteq \alpha\Big(\bigcup_{U \in \mathscr{U}} \beta(U)\Big) \subseteq \bigcap_{U \in \mathscr{U}} \alpha(\beta(U)) = \bigcap_{U \in \mathscr{U}} U = H\,.$$

The point is that each of the open subgroups U has finite index, and thus in each case $\alpha(\beta(U)) = U$ by the finite theory.

STEP 4. Finally, suppose that $\alpha(L) = \operatorname{Gal}(K/L) = H$, where L is some intermediate field. Let σ lie in G. Then from the diagram

$$\begin{tikzcd}
K \arrow[r, "\sigma"] \arrow[d, dash] & K \arrow[d, dash] \\
L \arrow[r, "\sigma"] \arrow[dr, dash] & \sigma(L) \arrow[d, dash] \\
 & F
\end{tikzcd}$$

we deduce that $\mathrm{Gal}(K/\sigma(L))=\sigma H\sigma^{-1}$. Thus according to parts (i)–(iii) above, we have that $\sigma(L)=L$ for all $\sigma\in G$ if and only if $\sigma H\sigma^{-1}=H$ for all $\sigma\in G$. This is to say that L is normal (and hence Galois) over F if and only if H is normal in G.□

REMARK. We leave it to the reader to determine the effect of $\alpha\circ\beta$ on an arbitrary subgroup of $\mathrm{Gal}(K/F)$. (See Exercise 15 below.)

1.4 Pro-p-Groups

Our aim here is to introduce for profinite groups an analogue of the p-Sylow subgroups that play such a crucial role in finite group theory. To begin, we must first generalize the notion of order.

Orders of Profinite Groups

DEFINITION. A *supernatural number* is a formal product

$$\prod_p p^{n_p}$$

where p runs over the set of rational primes and each $n_p\in\mathbf{N}\cup\{\infty\}$.

Clearly the set of supernatural numbers is a commutative monoid with respect to the obvious product. If a is a supernatural number, we set $v_p(a)$ equal to the exponent of p occurring in a. We say that *a divides b*, and as usual write $a|b$, if $v_p(a)\le v_p(b)$ for all primes p. Note that if $a|b$, there exists a supernatural number c such that $ac=b$.

Given supernatural numbers a and b, we may define both their *least common multiple* and *greatest common divisor* by the formulas

$$\mathrm{lcm}(a,b)=\prod p^{\sup(v_p(a),v_p(b))} \quad\text{and}\quad \gcd(a,b)=\prod p^{\inf(v_p(a),v_p(b))} \ .$$

One extends these notions to arbitrary (even) infinite families of supernatural numbers in the obvious way.

Now let G be a profinite group. As previously, let $\mathcal{N}$ denote the set of all open, normal subgroups of G. Recall that each quotient group G/N, for $N\in\mathcal{N}$, is finite.

DEFINITION. Let H be a closed subgroup of G. Then we define $[G:H]$, the *index of H in G*, by the formula

$$[G:H]=\operatorname*{lcm}_{N\in\mathcal{N}}\,[G/N:HN/N] \ .$$

In particular, $[G:\{e\}]$, the index of the trivial subgroup, is called the *order* of G and denoted $|G|$.

Using the standard isomorphism between HN/N and $H/H\cap N$, we may recast the definition above as

$$[G:H]=\operatorname*{lcm}_{N\in\mathcal{N}}\,[G/N:H/H\cap N] \ .$$

See also Exercise 16 below.

1-21 PROPOSITION. *Let G be a profinite group with closed subgroups H and K such that $H\subseteq K$. Then $[G:K]=[G:H][H:K]$.*

PROOF. Note that since H is closed, it is also profinite, and so the assertion is well defined. Now let N be any open normal subgroup of G. Then

$$[G/N:K/K\cap N]=[G/N:H/H\cap N]\,[H/H\cap N:K/K\cap N] \ . \tag{1.3}$$

The lcm (over $N\in\mathcal{N}$) of either side of the equation is, of course, $[G:H]$. Consider the factors on the right: if we replace N by any smaller subgroup $N_1\in\mathcal{N}$, both indices are inflated (cf. Exercise 17). Hence, taking intersections, any pair of prime powers occurring in $[G/N:H/H\cap N]$ and $[H/H\cap N:K/K\cap N]$, respectively, may be assumed to occur simultaneously. The upshot is that we can compute the lcm of the product by separately computing the lcm's of each factor. The first yields $[G:H]$; it remains only to show that the second yields $[H:K]$.

Let M be any open, normal subgroup of H. Then $M=H\cap U$, where U is open in G. But by Lemma 1-17, U contains an open, normal subgroup N of G, and one argues as above that

$$[H/M:K/K\cap M]\mid[H/H\cap N:K/K\cap N] \ .$$

Thus $[H:K]$ may be computed as the lcm over subgroups of H of the form $H\cap N$, where N is open and normal in G. Hence the second factor on the right of Eq. 1.3 indeed yields $[H:K]$, as required. □

REMARK. The proof shows that we may compute a profinite index as the lcm over any *cofinal* family $\mathcal{M}\subseteq\mathcal{N}$ of open normal subgroups of the ambient group; that is, if for every $N\in\mathcal{N}$ there exists an $M\in\mathcal{M}$ such that $M\subseteq N$, then

$$\operatorname*{lcm}_{N\in\mathcal{N}}\,[G/N:HN/N] \;=\; \operatorname*{lcm}_{M\in\mathcal{M}}\,[G/M:HM/M] \ .$$

EXAMPLES

(1) Consider the p-adic integers

$$\mathbf{Z}_p = \varprojlim_{n\geq 1}(\mathbf{Z}/p^n\mathbf{Z}) \ .$$

Let H_n denote the kernel of the projection map from $\mathbf{Z}_p$ to $\mathbf{Z}/p^n\mathbf{Z}$. Since this projection is surjective, we have $\mathbf{Z}_p/H_n \cong \mathbf{Z}/p^n\mathbf{Z}$, and it follows that p^∞ divides $|\mathbf{Z}_p|$. Conversely, every finite quotient of $\mathbf{Z}_p$ has order a power of p, and therefore $|\mathbf{Z}_p|=p^\infty$.

(2) Next consider

$$\hat{\mathbf{Z}} = \varprojlim_{n\geq 1}(\mathbf{Z}/n\mathbf{Z}) \ .$$

Arguing as above, every factor group $\mathbf{Z}/n\mathbf{Z}$ occurs as a quotient of $\hat{\mathbf{Z}}$, whence every positive integer is a divisor of its order. Thus

$$|\hat{\mathbf{Z}}| = \prod_{p \text{ prime}} p^\infty \ .$$

Pro-p-Groups

Let p be a rational prime. Recall that a group is called a *p-group* if the order of every element is finite and a power of p. In the case that G is finite, this is equivalent to the statement that the order of G is a power of p.

DEFINITION. A projective limit of finite p-groups is called a *pro-p-group*.

Of course, $\mathbf{Z}_p$ is a pro-p-group; so is $\hat{H}_p$, the projective limit of the Heisenberg groups $H(\mathbf{Z}/p^n\mathbf{Z})$. (See Exercise 18 below.)

1-22 PROPOSITION. *A profinite group G is a pro-p-group if and only if its order is a power of p (possibly infinite).*

PROOF. $\Leftarrow$) We have already seen in the proof of Theorem 1-14 that G is the projective limit of its finite quotient groups G/N. If the order of G is a power of p, then each of these quotients must be a p-group, as required.

$\Rightarrow$) Suppose that G is the projective limit of the projective system P_i of p-groups. Then by definition of the topology of G, cofinal among the open normal subgroups of G are subgroups of the form

$$M = (\textstyle\prod Q_i) \cap G$$

where $Q_i = P_i$ for all but finitely many indices, and $Q_i = \{e_i\}$ for the exceptions. Now given an arbitrary $x \in G$ and specifying any finite subset of its coordinates, there is clearly a finite exponent of the form $q=p^r$ such that x^q is trivial at each of the specified coordinates. Hence G/M is a p-group, and it follows by the remark following Proposition 1-21 that the order of G is a power of p. ❑

DEFINITION. Let G be a profinite group. A maximal pro-p-subgroup of G is called a *pro-p-Sylow subgroup* of G (or more simply, a *p-Sylow* subgroup of G).

Note that the trivial subgroup may well be a pro-p-subgroup of G for some primes p. The following theorem shows among other things that this is the case if and only if p does not divide the order of G.

1-23 THEOREM. *Let G be a profinite group and let p be a rational prime. Then the following assertions hold:*

(i) *p-Sylow subgroups of G exist.*

(ii) *Any pair of conjugate p-Sylow subgroups of G are conjugate.*

(iii) *If P is a p-Sylow subgroup of G, then $[G:P]$ is prime to p.*

(iv) *Each p-Sylow subgroup of G is nontrivial if and only if p divides the order of G.*

PROOF. As usual, let $\mathscr{N}$ denote the set of open normal subgroups of G and recall the explicit isomorphism

$$\begin{aligned} \varphi : G &\to \varprojlim G/N \\ x &\mapsto (xN)_{N\in\mathscr{N}} \ . \end{aligned}$$

Note in particular that if $x,y \in G$ and $xN=yN$ for every open normal subgroup N, then $x=y$. A similar statement holds for arbitrary subsets of G.

(i) For each $N\in\mathscr{N}$, let $\mathscr{P}(N)$ denote the set of p-Sylow subgroups of the finite group G/N. Then clearly $\mathscr{P}(N)$ is finite and, moreover, nonempty. (If G/N has order prime to p, then the trivial subgroup is a p-Sylow subgroup.) Assume that $M,N\in\mathscr{N}$ with $N\subseteq M$. Then there exists a surjective homomorphism of finite groups $\varphi_{M,N}: G/N \to G/M$. Since this map sends a p-Sylow subgroup of G/N to a p-Sylow subgroup of G/M (refer again to Exercise 17), we obtain an induced map $\varphi_{M,N}: \mathscr{P}(N) \to \mathscr{P}(M)$. Thus we obtain a projective system $(\mathscr{P}(N), \varphi_{M,N})$ of finite nonempty sets, and the projective limit of this system is likewise nonempty by Proposition 1-11. This means that there exists a projective system of

p-Sylow subgroups $(P_N, \varphi_{M,N})$, where for each $N \in \mathscr{N}$, we have $P_N \subseteq G/N$. Let P be the projective limit of the P_N, which we can clearly identify with a subgroup of the projective limit of the G/N and hence with a subgroup of G via φ. Then P is a pro-p-group by construction, and we shall now show that it is maximal. Let Q be any pro-p-subgroup containing P. Then for every open normal subgroup N, $QN/N \supseteq PN/N = P_N$. But Q is a pro-p-group, so by the previous proposition, QN/N is a p-group and therefore equal to the p-Sylow subgroup P_N. Thus for every open normal subgroup N, $QN/N = PN/N$, and therefore Q and P have the same image under φ and accordingly are equal. Hence P is indeed maximal, as claimed.

(ii) Let P and Q be p-Sylow subgroups of G. For every $N \in \mathscr{N}$, we make the following definitions:

$$\begin{aligned} P_N &= PN/N \\ Q_N &= QN/N \\ Y_N &= \{y_N \in G/N : y_N P_N y_N^{-1} = Q_N\} . \end{aligned}$$

Note that each Y_N is finite and, by the Sylow theorems for finite groups, nonempty. Moreover, the subsets Y_N clearly constitute a projective system. Let Y denote the (nonempty) projective limit of the Y_N, which we again identify with a subset of G via φ, and let y lie in Y. Then by construction, yPy^{-1} and Q have equal projection in G/N for all open, normal N and are therefore equal. Hence P and Q are indeed conjugate.

(iii) Let P be a p-Sylow subgroup of G. Then by definition

$$[G{:}P] = \operatorname*{lcm}_{N \in \mathscr{N}} [G/N{:}PN/N] .$$

But by Exercise 19, for each N, the subquotient PN/N is a p-Sylow subgroup of G/N, and so by finite group theory each index $[G/N{:}PN/N]$ is prime to p. Hence $[G{:}P]$ is likewise prime to p.

(iv) This follows at once from parts (i) and (iii). □

1-24 Corollary. *Let G be a commutative profinite group. Then the following assertions hold:*

(i) *For every prime p, G admits a unique pro-p-Sylow subgroup.*

(ii) *Let p and q be distinct primes and let P and Q be the corresponding Sylow subgroups. Then $P \cap Q$ is trivial.*

(iii) *G is isomorphic to the direct product of its Sylow subgroups.*

Proof. (i) In light of the commutativity of G, this follows at once from parts (i) and (ii) of the theorem above.

(ii) The order of $P \cap Q$ must divide powers of both p and q, whence this intersection must be trivial.

(iii) Let N be an open normal subgroup of G. Then for each pro-p-Sylow subgroup P we have a canonical projection from P onto PN/N, the unique p-Sylow subgroup of G/N. Note that this projection is trivial for all but the finitely many primes p that divide the order of G/N. By the theory of finite commutative groups, we have

$$\prod PN/N \cong G/N$$

where the product is taken over all of the Sylow subgroups of G. We may lift this isomorphism to G as follows:

$$\begin{aligned} G &= \underset{\leftarrow}{\lim}\, G/N \\ &= \underset{\leftarrow}{\lim} \prod PN/N \\ &= \prod \underset{\leftarrow}{\lim}\, PN/N \\ &= \prod \underset{\leftarrow}{\lim}\, P/P \cap N \\ &= \prod P . \end{aligned}$$

All products are over the set of Sylow subgroups of G; all projective limits are over the family of open, normal subgroups of G. The final line of the calculation is justified by the cofinality of subgroups of the form $P \cap N$ among the open subgroups of P, which may be deduced from Lemma 1-17. □

Example. Recall that the abelian profinite group

$$\hat{\mathbf{Z}} = \underset{\leftarrow}{\lim}\, \mathbf{Z}/n\mathbf{Z}$$

has order $\prod p^\infty$, where the product is taken over all primes. Given a prime p, let P be the unique corresponding p-Sylow subgroup of $\hat{\mathbf{Z}}$. Let P_n denote the unique p-Sylow subgroup of $\mathbf{Z}/n\mathbf{Z}$. Then

$$P = \underset{\underset{n}{\leftarrow}}{\lim}\, P_n = \underset{\underset{n}{\leftarrow}}{\lim}\, \mathbf{Z}/p^{v_p(n)}\mathbf{Z} = \underset{\underset{m}{\leftarrow}}{\lim}\, \mathbf{Z}/p^m\mathbf{Z} = \mathbf{Z}_p .$$

Thus according to the corollary, $\hat{\mathbf{Z}} = \prod \mathbf{Z}_p$.

Exercises

1. Let G be a topological group. Show that the topology on G is completely determined by a system of open neighborhoods of the identity e.

2. Let $G=\mathbf{Z}$ and impose the following topology: $U\subseteq G$ is open if either $0\notin U$ or $G-U$ is finite. Show that G is *not* a topological group with respect to this topology. [*Hint*: If so, the mapping $a\mapsto a+1$ would be a homeomorphism; show that it is not.]

3. This exercise shows that we may impose a nondiscrete topology on $\mathbf{Z}$ such that $\mathbf{Z}$ is nonetheless a topological group with respect to addition. Let S^1 denote the multiplicative group of complex numbers of absolute value 1. Recall that an element of $\mathrm{Hom}(\mathbf{Z},S^1)$ is called a *character* of $\mathbf{Z}$. We denote such a character χ. Let

$$\mathscr{G}=\prod_{\chi}S^1$$

where the product is taken over all characters. Then $\mathscr{G}$ is a compact topological group. Now consider the homomorphism

$$\begin{aligned} j:\mathbf{Z}&\to\mathscr{G}\\ n&\mapsto(\chi(n))\ . \end{aligned}$$

(a) Show that j is injective; that is, show that for any nonzero $n\in\mathbf{Z}$ there exists a character χ such that $\chi(n)\neq 1$.

(b) Let $G=j(\mathbf{Z})$. Then G is a group algebraically isomorphic to $\mathbf{Z}$ and a topological group with respect to the subspace topology induced by $\mathscr{G}$. Show that G is not discrete with respect to this topology and conclude that $\mathbf{Z}$ itself admits a nondiscrete topological group structure with respect to addition. [*Hint*: Suppose that $j(1)$ is open. Then there exists an open subset U of $\mathscr{G}$ such that $U\cap G=j(1)$; moreover, we may assume that all but finitely many projections of U onto its various coordinates yield all of S^1. Noting that $j(1)$ generates the infinite group G, one may now derive a contradiction.]

4. Give an example of a topological group with a closed subgroup that is *not* open.

5. Let X be a topological space and let $C(X)$ denote the space of connected components of X. (This constitutes a partition of X). As usual, we impose the quotient topology on $C(X)$—the strongest topology such that the canonical projection $\rho:X\to C(X)$ is continuous. Show that $C(X)$ is totally disconnected with respect to this topology. [*Hint*: We say that a subset Y of a topological space is *saturated* if whenever $y\in Y$, the entire connected component of y lies in Y. Let F be a connected component of $C(X)$ that contains more than one point. Show that $\rho^{-1}(F)$ is a saturated, closed, disconnected set. Write $\rho^{-1}(F)$ as the disjoint union of two saturated, closed subsets of X, and apply ρ to this decomposition to show that F is in fact disconnected—a contradiction.]

6. Let $G=\mathrm{GL}_n(\mathbf{R})$. Show that G° is the set of $n\times n$ matrices with positive determinant.

7. Let H be a subgroup of the topological group G. Show that its closure $\overline{H}$ is normal (respectively, abelian) if H is.

8. Let $f: G\to G'$ be a surjective continuous homomorphism of topological groups. Show that f factors uniquely through $G/\mathrm{Ker}(f)$; that is, there exists a unique continuous homomorphism $\bar{f}$ such that the following diagram commutes:

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\rho"'] & & G' \\ & G/\mathrm{Ker}(f) \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Show that $\bar{f}$ is moreover injective. Under what conditions is $\bar{f}$ a topological isomorphism onto its image?

9. Let $f:X\to Y$ be a continuous bijective mapping of topological spaces and assume that X is compact and Y is Hausdorff. Show that f is moreover a homeomorphism. [*Hint*: It suffices to show that f is open. What can one say about the image of U^c under f where U is any open subset of X?]

10. Let I be an index set with preordering defined by equality and let (G_i,φ_{ij}) be a projective system of sets defined with respect to I. What is the projective limit in this case?

11. Give an example of a projective system of finite nonempty sets over a preordered, but not directed, set of indices such that the projective limit is nevertheless itself empty.

12. Let G be an arbitrary group. Show that in general G is not isomorphic to the projective limit of the quotient groups G/N, as N varies over all of the

subgroups of G of finite index. Hence not every abstract group acquires a profinite structure by this device. [*Hint*: Take $G=\mathbf{Z}$.]

13. Let (G_i, φ_{ij}) and (H_i, φ_{ij}) be two projective systems of sets. (Note that we use the same map designators φ_{ij} for both systems.) Suppose that we have a family of maps $\{\zeta_i: G_i \to H_i\}$ that is compatible with these systems in the sense that $\varphi_{ij} \circ \zeta_j = \zeta_i \circ \varphi_{ij}$ for all pairs of indices $i \le j$. Show that there exists a unique map $\zeta: G \to H$ on their respective projective limits such that $\zeta_i \circ p_i = p_i \circ \zeta$ for all i, where p_i denotes the appropriate projection map. Observe that this construction works equally well in the categories of groups, topological spaces, and topological groups. [*Hint*: In light of the universal property of projective limits, consider the family of composed maps $\{\zeta_i \circ p_i: G \to H_i\}$.]

14. Let K/F be a Galois extension with Galois group G.

(a) Let L be an intermediate field that is finite over F. For any given $\sigma \in G$, define $N_L(\sigma) \subseteq G$ to be the set of $\tau \in G$ such that σ and τ agree on L. The subsets $N_L(\sigma)$ constitute a subbase for a topology on G. Show (i) that this topology remains unchanged if we restrict the subbase to normal intermediate fields that are finite over F and (ii) that this topology is identical to the profinite topology on G.

(b) Now let L be an arbitrary intermediate field, and let H denote the Galois group of K over L. Use the characterization of the profinite topology given in part (a) to show that the topology induced on H by G is identical to the profinite topology defined directly on H as Gal(K/L).

15. Let K/F be a Galois extension (not necessarily finite) and let H be any subgroup of $G=\mathrm{Gal}(K/F)$ (not necessarily closed). Let α and β be defined as in Theorem 1-20. Show that $\alpha\big(\beta(H)\big) = \overline{H}$, the closure of H.

16. Let G be a profinite group and let H be a closed subgroup. Show that

$$[G:H] = \operatorname*{lcm}_{N \in \mathscr{N}} [G:HN]$$

where $\mathscr{N}$ is the set of all open, normal subgroups of G. Show further that if M is any open subgroup of G containing H, then there exists an open normal subgroup N of G such that $M \supseteq NH$. Conclude from this and the previous equation that moreover,

$$[G:H] = \operatorname*{lcm}_{\substack{M \text{ open} \\ M \supseteq N}} [G:M] \ .$$

17. Let $\varphi: G \to G'$ be a surjective homomorphism of groups with kernel L. Let H be a subgroup of G of finite index and let H' be the image of H under φ. Show that $[G:H] = [G':H'] \cdot [HL:H]$.

18. For any commutative ring A with unity, define the *Heisenberg group* $H(A)$ over A by

$$H(A) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in A \right\} .$$

(a) Show that $H(A)$ is a group under multiplication in the matrix ring $M_3(A)$ and that this construction is, moreover, functorial in A.

To continue, for $n \ge 1$, $H(\mathbf{Z}/p^n\mathbf{Z})$ is clearly a group of order p^{3n}, and hence a p-group. If $m|n$, then by functoriality, we have that the canonical projection $\mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}/p^m\mathbf{Z}$ induces a homomorphism φ_{mn} from $H(\mathbf{Z}/p^n\mathbf{Z})$ to $H(\mathbf{Z}/p^m\mathbf{Z})$.

(b) Show that $(H(\mathbf{Z}/p^n\mathbf{Z}), \varphi_{mn})$ is a projective system of groups.

Let $\hat{H}_p$ denote the projective limit of the $H(\mathbf{Z}/p^n\mathbf{Z})$; by definition, this is a pro-p-group.

(c) Show that $H(\mathbf{Z}_p) \cong \hat{H}_p$. [*Hint*: Consider the map

$$\pi_n: H(\mathbf{Z}_p) \to H(\mathbf{Z}/p^n\mathbf{Z})$$

induced by projection from $\mathbf{Z}_p$ onto $\mathbf{Z}/p^n\mathbf{Z}$. Show that this is a continuous surjective homomorphism and that moreover, the family $\{\pi_n\}$ is compatible with the system of homomorphisms $\{\varphi_{mn}\}$. Finally, show that the map π obtained from the π_n by the universal property of the direct limit is the desired isomorphism.]

19. Let G be a profinite group and p a rational prime. For each open, normal subgroup N in G, let H_N be a p-subgroup of G/N (not necessarily a p-Sylow subgroup). Show that there exists a pro-p-Sylow subgroup P of G such that $PN/N \supseteq H_N$ for all N. Conclude (i) that every pro-p-subgroup of G is contained in a pro-p-Sylow subgroup of G; and (ii) that if P is a pro-p-Sylow subgroup of G, then PN/N is a p-Sylow subgroup of G/N for each open, normal subgroup N of G. [*Hint*: Generalize the argument from the proof of part (i) of Theorem 1-23.]