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

INTRODUCTION TO PROFINITE GROUPS

Luis Ribes
Carleton University, Ottawa, Canada

LECTURE 1

1.1 INFINITE GALOIS EXTENSIONS

1.2 THE KRULL TOPOLOGY

1.3 PROFINITE GROUPS

1.4 BASIC PROPERTIES OF PROFINITE GROUPS

1.5 PROFINITE GROUPS AS GALOIS GROUPS

1.6 SUPERNATURAL NUMBERS AND SYLOW SUBGROUPS

1.1 INFINITE GALOIS EXTENSIONS

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

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

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

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

defined by

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

then

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

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

$$\varphi \colon N \to N$$

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

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

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

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

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

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

we can defined a K-automorphism

$$\sigma\colon N \to N$$

by setting

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

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

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

and hence

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

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

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

1.2 THE KRULL TOPOLOGY

Although the above example shows that Theorem 1.1.1 does not hold for infinite Galois extension, it suggest a way of modifying the theorem so that it will in fact be valid even in those cases. The map σ of the example is in a sense approximated by the maps φ^{k_i}, since it coincides with φ^{k_i} on the subextension K_i which becomes larger and larger with increasing i, and $N = \bigcup_{i=1}^{\infty} K_i$. This leads to the idea of defining a topology in G so that in fact $\sigma = \lim \varphi^{k_i}$. Then σ would be in the closure of H and once could hope that G is the closure of H, suggesting a correspondence of the intermediate fields of N/K and the closed subgroups of G. In fact this is the case as we will see.

Definition 1.2.1 Let N/K be a Galois extension and $G = G_{N/K}$. The set

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

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

Remarks

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

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

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

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

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

since

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

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

For (ii): Consider the homomorphism

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

defined by

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

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

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

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

To see that h is continuous consider the composition

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

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

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

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

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

On the other hand

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

and if

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

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

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

and hence $h(G)$ is closed.

Finally h is open into $h(G)$, since if $L/K \in \mathcal{F}_n$,

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

which is open in $h(G)$.

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

Let

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

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

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

so $H = \{1\}$. □

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

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

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

so

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

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

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

Consider the epimorphism

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

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

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

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

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

On the other hand, let $\sigma \bigcap_{U \in \mathcal{S}} H \cdot U$; then $U \in \mathcal{S} \Rightarrow \sigma U \cap H \neq \emptyset$; so every neighborhood of σ hits H; hence $\sigma \in H$. Thus H is the intersection of the open subgroups $H \cdot U$, $U \in \mathcal{S}$. □

We are now in a position to generalize Theorem 1.1.1 to infinite Galois extensions.

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

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

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

Proof. Since $\Phi(L) = G_{N/L}$ is compact (Prop. 1.2.2), it is closed in G; so Φ is in fact a map into $\{G : 1\}$. Define

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

by

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

Clearly Proposition 1.1.2 is still valid and we have $\Psi \circ \Phi = \mathrm{id}_{\{N:K\}}$. Now we prove that $\Phi \circ \Psi = \mathrm{id}_{\{G:1\}}$. If L/K is finite,

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

If $H \in \{G : 1\}$, then, by Proposition 1.2.3,

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

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

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

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

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

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

1.3 PROFINITE GROUPS

Let $I = (I, \preceq)$ denote a *directed partially ordered set* or *directed poset*, that is, I is a set with a binary relation $\preceq$ satisfying the following conditions:

(a) $i \preceq i$, for $i \in I$;

(b) $i \preceq j$ and $j \preceq k$ imply $i \preceq k$, for $i, j, k \in I$;

(c) $i \preceq j$ and $j \preceq i$ imply $i = j$, for $i, j \in I$; and

(d) if $i, j \in I$, there exists some $k \in I$ such that $i, j \preceq k$.

An *inverse* or *projective system* of topological spaces (respectively, topological groups) over I, consists of a collection $\{X_i \mid i \in I\}$ of topological spaces (respectively, topological groups) indexed by I, and a collection of continuous mappings (respectively, continuous group homomorphisms) $\varphi_{ij} : X_i \longrightarrow X_j$, defined whenever $i \succeq j$, such that the diagrams of the form

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

commute whenever they are defined, i.e., whenever $i, j, k \in I$ and $i \succeq j \succeq k$. In addition we assume that φ_{ii} is the identity mapping id_{X_i} on X_i. We denote such a system by $\{X_i, \varphi_{ij}, I\}$.

The *inverse limit* or *projective limit*

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

of the inverse system $\{X_i, \varphi_{ij}, I\}$ is the subspace (respectively, subgroup) X of the direct product

$$\prod_{i \in I} X_i$$

of topological spaces (respectively, topological groups) consisting of those tuples (x_i) that satisfy the condition $\varphi_{ij}(x_i) = x_j$ if $i \succeq j$. We assume that X has the topology induced by the product topology of $\prod_{i \in I} X_i$. For each $i \in I$, let

$$\varphi_i : X \longrightarrow X_i$$

denote the restriction of the canonical projection $\prod_{i \in I} X_i \longrightarrow X_i$. Then one easily checks that each φ_i is continuous (respectively, a continuous homomorphism), and $\varphi_{ij}\varphi_i = \varphi_j$ $(j \prec i)$. The space (respectively, topological group) X together with the maps (repsectivel, homomorphisms) φ_i satisfy the following universal property that in fact **characterizes** (as one easily checks) the inverse limit:

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

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

commutes.

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

- (i) The collection of all finite groups;
- (ii) the collection of all finite p-groups (for a fixed prime p);
- (iii) the collection of all finite nilpotent groups.

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

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

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

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

1.3.2 Examples

(a) The Galois group $G_{N/K}$ of a Galois extension N/K of fields.

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

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

Make $\mathcal{N}$ into a directed poset by defining $M \preceq N$ if $M \geq N$ $(M, N \in \mathcal{N})$. If $M, N \in \mathcal{N}$ and $N \succeq M$, let $\varphi_{NM} : G/N \longrightarrow G/M$ be the natural epimorphism. Then

$$\{G/N, \varphi_{NM}\}$$

is an inverse system of groups in $\mathcal{C}$, and we say that the pro-$\mathcal{C}$ group

$$G_{\hat{\mathcal{C}}} = \varprojlim_{N \in \mathcal{N}} G/N$$

is the *pro-$\mathcal{C}$ completion* of G. In particular we use the terms *profinite completion*, the *pro-p completion*, the *pronilpotent completion*, etc., in the cases where $\mathcal{C}$ consists of all finite groups, all finite p-groups, all finite nilpotent groups, etc., respectively.

The profinite and pro-p completions of a group of G appear quite frequently, and they will be usually denoted instead by $\widehat{G}$, and $G_{\hat{p}}$ respectively.

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

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

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

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

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

1.3.3 Lemma *Let*

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

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

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

be the projection homomorphisms. Then

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

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

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

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

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

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

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

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

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

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

□

1.3.4 Theorem (Topological characterizations of pro-$\mathcal{C}$ groups)
The following conditions on a topological group G are equivalent.

(a) *G is a pro-$\mathcal{C}$ group.*

(b) *G is compact, Hausdorff, totally disconnected, and for each open normal subgroup U of G, $G/U \in \mathcal{C}$.*

(c) *The identity element 1 of G admits a fundamental system $\mathcal{U}$ of open neighborhoods U such that each U is a normal subgroup of G with $G/U \in \mathcal{C}$, and*

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

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

1.4 BASIC PROPERTIES OF PROFINITE GROUPS

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

1.4.1 Lemma

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

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

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

The proof of this lemma is an easy exercise using the characterizations in Theorem 1.3.4. For a formal proof of this theorem, see [RZ], Propositions 2.1.4 and 2.2.1.

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

1.4.2 Proposition *Let $K \leq H$ be closed subgroups of a pro finite group G . Then there exists a continuous section*

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

such that $\sigma(1H) = 1K$.

Proof. We consider two cases.

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

$$p_i \colon x_iUK \to x_iUH/H$$

$i = 1, 2, \ldots, n$, defined as restrictions of p, are homeomorphisms. Then it will follow that $\sigma = \bigcup_{i=1}^{n} p_i^{-1}$ will be the desired section. It is plain that p_i is a continuous surjection. On the other hand if $p_i(x_iu_1) = p_i(x_iu_2)$, $(u_1, u_2 \in U)$, then $x_iu_1u_2^{-1}x_i^{-1} \in H$. But since U is normal, $x_iu_1u_2^{-1}x_i^{-1} \in U$, and hence $x_iu_1u_2^{-1}x_i^{-1} \in H \cap U \leq K$. Thus x_iu_1 and x_iu_2 represent the same element in x_iUK, i.e., p is injective. Since x_iUK is compact, p must be a homeomorphism.

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

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

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

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

which is also injective, for

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

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

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

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

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

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

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

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

1.5 PROFINITE GROUPS AS GALOIS GROUPS

Together with Theorem 1.2.4, the following result provides a new characterization of profinite groups.

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

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

If $k \in K$, consider the subgroup

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

of G. If the indeterminates that appear in the rational expression of k are $\{t_i \in G/U_i \mid i = 1, \ldots, n\}$, then

$$G_k \supseteq \bigcap_{i=1}^{n} U_i.$$

Therefore G_k is an open subgroup of G, and hence of finite index. From this we deduce that the orbit of k under the action of G is finite. Say that $\{k = k_1, k_2, \ldots, k_r\}$ is the orbit of k. Consider the polynomial

$$f(X) = \prod_{i=1}^{r} (X - k_i).$$

Since G transforms this polynomial into itself, its coefficients are in L, that is, $f(X) \in L[X]$. Hence k is algebraic over L. Moreover, since the roots of $f(X)$ are all different, k is separable over L. Finally, the extension $L(k_1, k_2, \ldots, k_r)/L$ is normal. Hence K is a union of normal extensions over L; thus K/L is a normal extension. Therefore K/L is a Galois extension. Let H be the Galois group of K/L; then G is a subgroup of H. To show that $G = H$, observe first that the inclusion mapping $G \hookrightarrow H$ is continuous, for assume that $U \triangleleft_o H$ and let K^U be the subfield of the elements fixed by U; then K^U/L is a finite Galois extension by Theorem 1.2.4; say, $K^U = L(k'_1, \ldots, k'_s)$ for some $k'_1, \ldots, k'_s \in K$. Then

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

Therefore $G \cap U$ is open in G. This shows that G is a closed subgroup of H. Finally, since G and H fix the same elements of K, it follows from Theorem 1.2.4 that $G = H$. $\square$

1.6 SUPERNATURAL NUMBERS AND SYLOW SUBGROUPS

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

A *supernatural number* is a formal product

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

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

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

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

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

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

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

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

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

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

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

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

1.6.1 Proposition *Let G be a profinite group.*

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

(b) *If $H \le_c G$, then*
$$[G : H] = \mathrm{lcm}\{[G : U] \mid H \le U \le_o G\};$$

(c) *If $H \le_c G$ and $\mathcal{U}'$ is a fundamental system of neighborhoods of 1 in G consisting of open normal subgroups, then*
$$[G : H] = \mathrm{lcm}\{[G/U : HU/U] \mid U \in \mathcal{U}'\};$$

(d) *Let $K \le_c H \le_c G$. Then*
$$[G : K] = [G : H][H : K];$$

(e) *Let $\{H_i \mid i \in I\}$ be a family of closed subgroups of G filtered from below. Assume that $H = \bigcap_{i\in I} H_i$. Then*
$$[G : H] = \mathrm{lcm}\{[G : H_i] \mid i \in I\};$$

(f) *Let $\{G_i, \varphi_{ij}\}$ be a surjective inverse system of profinite groups over a directed poset I. Let $G = \varprojlim_{i\in I} G_i$. Then*
$$\#G = \mathrm{lcm}\{\#G_i \mid i \in I\};$$

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

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

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

1.6.2 Proposition *Let $\{X_i, \varphi_{ij}\}$ be an inverse system of compact Hausdorff nonempty topological spaces X_i over the directed set I. Then*

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

is nonempty. In particular, the inverse limit of an inverse system of nonempty finite sets is nonempty.

Proof. For each $j \in I$, define a subset Y_j of $\prod X_i$ to consist of those (x_i) with the property $\varphi_{jk}(x_j) = x_k$ whenever $k \preceq j$. Using the axiom of choice, one easily checks that each Y_j is a nonempty closed subset of $\prod X_i$. Observe that if $j \preceq j'$, then $Y_j \supseteq Y_{j'}$; it follows that the collection of subsets $\{Y_j \mid j \in I\}$ has the finite intersection property (i.e., any intersection of finitely many Y_j is nonempty), since the poset I is directed. Then, one deduces from the compactness of $\prod X_i$ that $\bigcap Y_j$ is nonempty. Since

$$\varprojlim_{i \in I} X_i = \bigcap_{j \in I} Y_j.$$

the result follows. □

1.6.3 Theorem *Let p be a fixed prime number and let*

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

be a profinite group, where $\{G_i, \varphi_{ij}, I\}$ is a surjective inverse system of finite groups. Then

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

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

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

Proof.

(a) Let $\mathcal{H}_i$ be the set of all p-Sylow subgroups of G_i. Then $\mathcal{H}_i \neq \emptyset$. Since $\varphi_{ij} : G_i \to G_j$ is an epimorphism, $\varphi_{ij}(\mathcal{H}_i) \subset \mathcal{H}_j$, whenever $i \succeq j$. Therefore, $\{\mathcal{H}_i, \varphi_{ij}, I\}$ is an inverse system of nonempty finite sets. Consequently, according to Proposition 1.6.2,

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

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

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

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

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

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

and $S = \varprojlim S_i$ is a p-Sylow subgroup of G.

(c) Let H and K be p-Sylow subgroups of G. Then $\varphi_i(H)$ and $\varphi_i(K)$ are p-Sylow subgroups of G_i ($i \in I$), and so they are conjugate in G_i. Let

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

Clearly $\varphi_{ij}(Q_i) \subseteq Q_j$ ($i \succeq j$). Therefore, $\{Q_i, \varphi_{ij}\}$ is an inverse system of nonempty finite sets. Using again Proposition 1.6.2, let $q \in \varprojlim Q_i$. Then $q^{-1}Hq = K$, since $\varphi_i(q^{-1}Hq) = \varphi_i(K)$, for each $i \in I$. □