Profinite Groups 1

John S. Wilson

E-mail: wilson@math.uni-leipzig.de

What is a profinite group?

– a compact Hausdorff totally disconnected group

– a closed subgroup of a Cartesian product of finite groups

– an inverse limit of finite groups

– a Galois group of an algebraic field extension.

(Totally disconnected: no connected subset has more than one element.

A [locally] compact Hausdorff space is totally disconnected iff its compact open subsets form a base for its topology.)

What is ~~a profinite group~~ a pro-p group?

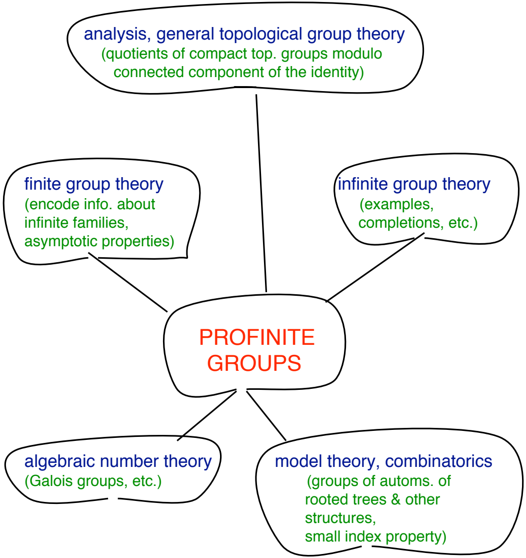
– a compact Hausdorff tot. disconnected group in which $g^{p^n} \to 1$ as $n \to \infty$, for all $g \in G$

– a closed subgroup of a Cartesian product ~~of finite groups~~ of finite p-groups

– an inverse limit o~~f finite grou~~ps of finite p-groups

– a Galois group of an algebraic field extension such that each finite subextension has p-power degree.

Where do profinite groups arise?



If X, Y are groups, so is $X \times Y$: $\quad (x_1, y_1)(x_2, y_2) = (x_1 x_2, y_2 y_2)$.
If X, Y are top. spaces so is $X \times Y$: base of open sets $\{U \times V \mid U \text{ open in } X,\ V \text{ open in } Y\}$.
Let G be both a group and a top. space: G is a topological group if both $x \mapsto x^{-1}$ and $(x, y) \mapsto xy$ (from $G \times G$ to G) are continuous.
If X, Y are top. groups, so is $X \times Y$.

Infinite Products. $C = \mathrm{Cr}_{\lambda \in \Lambda} X_\lambda$ is the Cartesian product of $(X_\lambda \mid \lambda \in \Lambda)$.
Elements are vectors $(x_\lambda)_{\lambda \in \Lambda}$, entries indexed by Λ.
Projection maps $\pi_\lambda : C \to X_\lambda$.
If each X_λ is a group so is C: $\quad (x_\lambda)(y_\lambda) = (x_\lambda y_\lambda)$.
If each X_λ is a top. space, so is C: subbase of open sets $\{\pi_\lambda^{-1}(U_\lambda) \mid \lambda \in \Lambda, U_\lambda \text{ open in } X_\lambda\}$.
If each X_λ is a top. group, so is C.

Tychonoff's theorem. If each X_λ is compact then so is C.

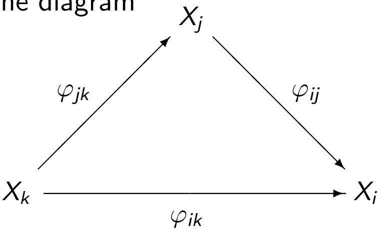
So if each X_λ is compact Hausdorff, so is each closed subset of C.
If X_λ is a cpct. Haus. top. group, so is each closed subgroup of C.
(E.g., take X_λ finite, with discrete top.)

Inverse systems

A directed set is a poset I such that for all $i_1, i_2 \in I$ there is an element $j \in I$ for which $i_1 \leqslant j$ and $i_2 \leqslant j$.

(1.1.1) Definition. An inverse system $(X_i, \varphi_{ij})_I$ of top. spaces indexed by a directed set I is a family $(X_i \mid i \in I)$ of top. spaces with a family $(\varphi_{ij}\colon X_j \to X_i \mid i, j \in I,\ i \leqslant j)$ of conts. maps such that $\varphi_{ii} = \mathrm{id}_{X_i}$ for each i and $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ whenever $i \leqslant j \leqslant k$.

So for $i \leqslant j \leqslant k$ the diagram



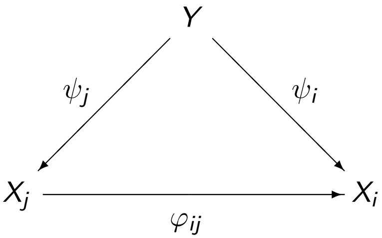
commutes.

Sets with no specified topology are given the discrete topology.

If (X_i, φ_{ij}) consists of top. groups and conts. homoms., (X_i, φ_{ij}) is an inverse system of top. groups; similarly for top. rings.

Inverse limits

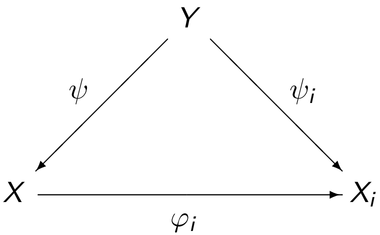
Let $(X_i, \varphi_{ij})_I$ be an inverse system of top. spaces, Y a top. space. A family $(\psi_i \colon Y \to X_i \mid i \in I)$ of conts. maps is compatible if $\varphi_{ij}\psi_j = \psi_i$ for $i \leqslant j$. That is, each diagram



is commutative.

(1.1.3) Definition. An inverse limit (X, φ_i) of an inverse system $(X_i, \varphi_{ij})_I$ of top. spaces (resp. groups, rings) is a top. space (resp. group, ring) X together with a compatible family $(\varphi_i\colon X \to X_i)$ of conts. maps (resp. conts. homoms.) with the foll. universal property (UP):

for each compatible family $(\psi_i\colon Y \to X_i)$ of conts. maps from a space Y (resp. conts. homoms. from a group or ring Y), there is a unique conts. map (resp. conts. homom.) $\psi\colon Y \to X$ such that $\varphi_i \psi = \psi_i$ for each i.
That is, there is a unique ψ such that the foll. diagrams are commutative.



Existence and 'uniqueness'

(1.1.4) Let $(X_i, \varphi_{ij})_I$ be an inverse system.

(a) If $(X^{(1)}, \varphi_i^{(1)})$ and $(X^{(2)}, \varphi_i^{(2)})$ are inverse limits, then $\exists$ isom. $\bar{\varphi}\colon X^{(1)} \to X^{(2)}$ such that $\varphi_i^{(2)}\bar{\varphi} = \varphi_i^{(1)}$ for each i. (If (X_i, φ_{ij}) is an inverse system of spaces then $\bar{\varphi}$ is just a homeom.)

(b) Write $C = \mathrm{Cr}(X_i \mid i \in I)$ and π_i for the projection $C \to X_i$. Define

$$X = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c) \text{ for all } i, j \text{ with } j \geqslant i\}$$

and $\varphi_i = \pi_i|_X$ for each i. Then (X, φ_i) is an inverse limit of (X_i, φ_{ij}).

(c) If (X_i, φ_{ij}) is an inverse system of top. groups and conts. homoms., then X is a top. group and the maps φ_i are conts. homoms.

So the inverse limit of $(X_i, \varphi_{ij})_I$ exists and is unique up to isom. Call it the inverse limit, write $\varprojlim (X_i, \varphi_{ij})$, or just $\varprojlim X_i$.
Write $s \varprojlim X_i$ for the inverse limit constructed above as subgroup of C.

Note. If $(X_i, \varphi_{ij})_I$ is an inverse system of top. groups, then from (b) its inverse limit, as a set, is also the inverse limit of (X_i, φ_{ij}) as an inverse system of sets.

(0.3.4) Let $(G_\lambda \mid \lambda \in \Lambda)$ be top. groups, and

$$C = \mathrm{Cr}(G_\lambda \mid \lambda \in \Lambda) .$$

Define multiplication in C pointwise ($(x_\lambda)(y_\lambda) = (x_\lambda y_\lambda)$). Then C is a topological group, i.e., mult. and inversion are conts. maps.

Proof: definition of product topology plus

Claim. A map $f\colon Z \to C$ is conts. $\Leftrightarrow$ each $\pi_\lambda f$ is continuous.
$\Rightarrow$ klar.
Suppose each $\pi_\lambda f$ conts. If U_i is open in X_{λ_i} for $i = 1, \ldots, n$ then each $(\pi_{\lambda_i} f)^{-1}(U_i)$ is open in Z so
$f^{-1}(\bigcap_{i=1}^n \pi_{\lambda_i}^{-1}(U_i)) = \bigcap_{i=1}^n (\pi_{\lambda_i} f)^{-1}(U_i)$ is open in Z.

Topological basics 1

If $f\colon X \to Y$ and $g\colon Y \to Z$ are conts. so is $gf\colon X \to Z$.
A bijection $f\colon X \to Y$ is a homeomorphism iff f, f^{-1} are both conts.

(0.1.2)
(a) Each closed subset of a compact space is compact.
(b) Each compact subset of a Hausdorff space is closed.
(c) If $f\colon X \to Y$ is continuous and X is compact then $f(X)$ is compact.
(d) If $f\colon X \to Y$ is continuous and bijective and if X is compact and Y is Hausdorff then f is a homeomorphism.
(e) If $f\colon X \to Y$ and $g\colon X \to Y$ are continuous and Y is Hausdorff then $\{x \in X \mid f(x) = g(x)\}$ is closed in X.

(0.1.3) Let X be a totally disconnected space. Then $\{x\}$ is closed in X, for each $x \in X$.

Products of topological spaces

Let $C = \mathrm{Cr}(X_\lambda \mid \lambda \in \Lambda)$ be the product of spaces X_λ. The projection map π_λ takes (x_λ) to x_λ.
The open sets in the product top. are the unions of sets

$$\pi_{\lambda_1}^{-1}(U_1) \cap \cdots \cap \pi_{\lambda_n}^{-1}(U_n) \qquad (*)$$

with n finite, each λ_i in Λ and U_i open in X_{λ_i}. So each projection π_λ is continuous (prod. top. is minimal with this property).

Remark. Let $a = (a_\lambda) \in C$ and let N be an open neighbourhood of a in C. Thus N contains a set S of form $(*)$ with $a \in S$, so there exist $\lambda_1, \ldots, \lambda_n \in \Lambda$ and open $U_i \subseteq X_{\lambda_i}$ with $a_{\lambda_i} \in U_i$ for each i and with $\pi_{\lambda_1}^{-1}(U_1) \cap \cdots \cap \pi_{\lambda_n}^{-1}(U_n) \subseteq N$. In particular, N contains

$$\{x \in C \mid \pi_{\lambda_1}(x) = a_{\lambda_1}, \ldots, \pi_{\lambda_n}(x) = a_{\lambda_n}\}\,.$$

(0.2.1) Let $(X_\lambda \mid \lambda \in \Lambda)$ be a family of top. spaces, C their Cartesian product.
(a) If each X_λ is Hausdorff, so is C.
(b) If each X_λ is totally disconnected, so is C.
(c) If each X_λ is compact, so is C.

Proof. (a) and (b) are elementary; in (b), since a conts. image of a connected set is connected, the projection in each X_λ of a non-empty connected set has one element.

(c) is Tychonoff's Theorem, postponed.

Topology of inverse limits

(1.1.5) Let $(X_i, \varphi_{ij})_I$ be an inverse system and write $X = \varprojlim X_i$.

(a) If each X_i is Hausdorff, so is X.
(b) If each X_i is totally disconnected, so is X.
(c) If each X_i is Hausdorff, then $s \varprojlim X_i$ is closed in

$$C = \mathrm{Cr}(X_i \mid i \in I).$$

(d) If each X_i is compact and Hausdorff, so is X.
(e) If each X_i is a non-empty compact Hausdorff space, then $X \neq \emptyset$.

(1.1.6) Let (X, φ_i) be an inverse limit of an inverse system $(X_i, \varphi_{ij})_I$ of non-empty compact Hausdorff spaces. Then
(a) $\varphi_i(X) = \bigcap_{j \geqslant i} \varphi_{ij}(X_j)$ for each $i \in I$.
(b) the sets $\varphi_i^{-1}(U)$ with $i \in I$ and U open in X_i form a base for the topology on X.
(c) if $Y \subseteq X$ and $\varphi_i(Y) = X_i$ for each i then Y is dense in X.
(d) If Y is a top. space and θ is a map $Y \to X$ then θ is conts. iff each $\varphi_i \theta$ is conts.
(e) If A is discrete and $f\colon X \to A$ is a conts., then f factors through some X_i, i.e., $\exists\ i$ and conts. $g\colon X_i \to A$ with $f = g\varphi_i$.

Quotients

Let ρ be an equivalence relation on a top. space X.
X/ρ is the quotient set (elements the equiv. classes)
q the quotient map $X \to X/\rho$ (maps $x \in X$ to its equiv. class).
The quotient topology on X/ρ has as open sets all $V \subseteq X/\rho$ such that $q^{-1}(V)$ is open in X.
Then q is continuous. Easy to check the following:

if $f\colon X \to Z$ is a continuous map to a space Z such that ρ-equiv. elements have the same image under f, then there is a unique continuous map $f^*\colon X/\rho \to Z$ such that $f = f^*q$.

Call a subspace of a top. clopen if it is closed and open.

(1.1.7) Let X be a compact Hausdorff totally disconnected space. Then X is the inverse limit of its discrete quotient spaces.

(1.4.1) Let G be a group, $\mathcal{L}$ a non-empty family of normal subgroups such that if $K_1, K_2 \in \mathcal{L}$ and $K_1 \cap K_2 \leqslant K_3 \triangleleft G$ then $K_3 \in \mathcal{L}$. Let $\mathcal{T}$ be the family of all unions of sets of cosets Kg with $K \in \mathcal{L}, g \in G$. Then
(a) $\mathcal{T}$ is a topology on G and G is a top. group;
(b) $\mathcal{L}$ is the set of open normal subgroups of G wrt this topology.