Algebraic Number Theory – Lecture 15

Sandro Bettin

"Only two things are infinite, the universe and human stupidity, and I'm not sure about the former."

– Albert Einstein

Definitions.

- A directed system is an ordered set I in which for each pair $i, j \in I$ there exists a $k \in I$ such that $i \leqslant k$, $j \leqslant k$.
- A projective system over a directed system I is the set of pairs
$$\{(X_i, f_{i,j}) \mid i, j \in I, i \leqslant j\}$$
where the X_i are topological spaces and the $f_{i,j}$ are continuous maps
$$f_{i,j} : X_j \longrightarrow X_i$$
such that one has
$$f_{i,i} = id_{X_i},$$
$$f_{i,k} = f_{i,j} \circ f_{j,k}, \text{ when } i \leqslant j \leqslant k.$$
- The projective (or inverse) limit
$$X = \varprojlim_{i \in I} X_i$$
of a projective system $\{(X_i, f_{i,j})\}_{i \leqslant j}$, is defined to be the subset
$$X = \{(x_i)_{i \in I} \in \prod_{i \in I} X_i \mid f_{i,j}(x_j) = x_i \text{ for } i \leqslant j\}$$
of the product $\prod_{i \in I} X_i$ equipped with the product topology (i.e. the open sets of $\prod_{i \in I} X_i$ are of the form $\prod_{i \in I} A_i$, where A_i is open in X_i and $A_i = X_i$ for all but a finite number of indices i).

Remarks.

1) If the topological spaces $\{X_i\}_{i \in I}$ are also groups then we require that the $f_{i,j}$ are also group homomorphisms. It's easy to see that the projective limit, equipped with the multiplication induced by the componentwise multiplication, is a topological group. The analogous result holds if the $\{X_i\}_{i \in I}$ are rings, modules, ...
2) One can define, in a similar way, the inductive (or direct) limit, the categorical dual of the projective limit.

Examples.

1) Let p be a prime, $I = \mathbb{N}$ and $X_n = \mathbb{Z}/p^n\mathbb{Z}$. Let $f_{m,n}$ for $n \geqslant m$ be the reduction modulo p^m
$$f_{m,n} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}.$$
The projective limit
$$\mathbb{Z}_p := \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$
is the ring of the p-adic integers.
2) Let $I = \mathbb{N}$, with order given by divisibility (i.e. $n \leqslant m$ iff $n|m$), $X_n = \mathbb{Z}/n\mathbb{Z}$ and $f_{n,m}$ for $n|m$ be the reduction modulo m. The projective limit
$$\hat{\mathbb{Z}} := \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$$
is the Prüfer ring.

Proposition 1. *For a topological group G, the followings are equivalent:*

i) *G is the projective limit of finite groups, each equipped with the discrete topology;*
ii) *G is compact and totally disconnected (i.e. the only connected subsets are the singletons);*
iii) *G is Hausdorff, compact and admits a basis of neighbourhoods of 1 consisting of normal subgroups;*
iv) *G is compact and*

$$G \cong \varprojlim_{N \lhd G,\, open} G/N;$$

v) *G is isomorphic to a closed subgroup of a cartesian product of finite groups, each equipped with the discrete topology.*

Proof.
i) $\Rightarrow$ *iii)* Let

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

with the G_i finite groups with the discrete topology. Since the G_i are Hausdorff and compact so is their product $\prod_{i \in I} G_i$ (by Tykhonov's theorem). Moreover, G is given by

$$G = \bigcap_{i \leqslant j} \left\{ (x_k)_k \in \prod_k G_k \mid f_{i,j}(x_j) = x_i \right\},$$

and so it's a closed and hence compact subset of $\prod_{i \in I} G_i$. Now, let A be an open neighbourhood of 1, since A is open it must has the form

$$A = G \cap \prod_i A_i,$$

with A_i open neighbourhoods of 1 in G_i and $A_i \neq G_i$ only for i in a finite subset $J \subset I$. Since the G_i are equipped with the discrete topology, the subset

$$\prod_{i \in J} \{1\} \times \prod_{i \in I \setminus J} G_i \subset \prod_i G_i$$

is an open neighbourhood of 1 for $\prod_i G_i$ contained in $\prod_i A_i$ and it's also a normal subgroup. Hence the set

$$G \cap \prod_{i \in J} 1 \times \prod_{i \in I \setminus J} G_i \subset G$$

is an open neighbourhood of 1 for G contained in A and it's also a normal subgroup. Thus G admits a basis of neighbourhoods of 1 consisting of normal subgroups.
iii) $\Rightarrow$ *ii)* Let G be Hausdorff, compact and with a basis of neighbourhoods of 1 consisting of normal subgroups and let D be a subset of G with at least two elements a_1 and a_2. Since G is Hausdorff, there exists a normal subgroup $N \lhd G$ such that $a_1 N \cap a_2 N = \emptyset$. The cosets gN for $g \in G$ are open and cover G and so the set $\{gN \mid g \in G\}$ has a finite number of elements, thus we have that $a_1 N \cap D$ and

$$\bigcup_{\substack{a \in N, \\ aN \neq a_1 N}} aN \cap D$$

are disjoint, non-empty and open sets of A whose union is A. Therefore A is disconnected.
ii) $\Rightarrow$ *iii)* Let G be a compact and totally disconnected topological group (and hence Hausdorff). We have that

$$\bigcap_{\substack{N \lhd G \\ N \text{ open}}} N = \{1\} \tag{1}$$

(see Bourbaki - Topologie gnrale). Now, let A be an open neighbourhood of 1 and assume that there isn't any open (and hence closed) $N \triangleleft G$ contained in A. Therefore $N_1 \cap \cdots \cap N_r \cap (G \setminus A)$ is closed and non empty for any open $N_1, \ldots, N_r \triangleleft G$. Thus, since G is compact we have

$$\bigcap_{\substack{N \triangleleft G \\ N \text{ open}}} N \cap (G \setminus A) \neq \emptyset$$

and that's a contradiction by (1).

iii) $\Rightarrow$ *iv)* The projection

$$G \longrightarrow \varprojlim_{N \triangleleft G, \text{ open}} G/N$$

is injective since it has kernel

$$\bigcap_{\substack{N \triangleleft G \\ N \text{ open}}} N = \{1\}.$$

Moreover, the projection is continuous and its image is dense (exercise) and so it has to be surjective since G is compact.

iv) $\Rightarrow$ *i)* Trivial, since every open subgroup of a compact group has finite index.

i) $\Rightarrow$ *v)* Trivial.

v) $\Rightarrow$ *ii)* Trivial, since by Tykhonov's theorem the cartesian product of compact sets is compact. □

Definition. A topological group that satisfies one of the conditions of the previous proposition is called a profinite group.

Remarks.

- Given a group G the profinite group
$$\widehat{G} := \varprojlim_{\substack{N \triangleleft G, \\ G/N \text{ finite}}} G/N$$
is called the completion of G and it has G as a dense subgroup. Note that even if G is profinite, it's not always true that $G \cong \widehat{G}$.
- Given a class C of finite groups (such as finite cyclic groups, finite p-groups, ...) one can define the pro-C-groups in a similar way, that is as projective limits of C-groups. If C has some good property the analogue of the previous proposition holds.

Examples.

1) $\mathbb{Z}_p$ is a profinite group. Moreover, it's a pro-cyclic and pro-p group and it's the pro-p-completion of $\mathbb{Z}$.
2) $\hat{\mathbb{Z}}$ is the profinite and pro-cyclic completion of $\mathbb{Z}$.
3) For any algebraic Galois extension Ω/K the Galois group $\mathrm{Gal}(\Omega/K)$ carries a canonical topology called the Krull topology, it can be defined by stating that the set
$$\{\mathrm{Gal}(L/K) \mid L/K \text{ is a finite Galois subextension of } \Omega/K\}$$
is a basis of neighbourhood of 1. By construction $\mathrm{Gal}(\Omega/K)$ has a basis of neighbourhoods of 1 consisting of normal subgroups, moreover it turns out that with this topology it is also compact and Hausdorff and therefore it is a profinite group.