Profinite Groups

Hendrik Lenstra

1. Introduction

We begin informally with a motivation, relating profinite groups to the p-adic numbers. Let p be a prime number, and let $\mathbb{Z}_p$ denote the ring of p-adic integers, namely, the completion of $\mathbb{Z}$ under the p-adic metric. Any element $\gamma \in \mathbb{Z}_p$ has a unique p-adic expansion

$$\gamma = c_0 + c_1 p + c_2 p^2 + \cdots = (\ldots c_3 c_2 c_1 c_0)_p,$$

with $c_i \in \mathbb{Z}$, $0 \leq c_i \leq p-1$, called the *digits* of γ. This ring has a topology given by a restriction of the product topology—we will see this below.

The ring $\mathbb{Z}_p$ can be viewed as $\mathbb{Z}/p^n\mathbb{Z}$ for an 'infinitely high' power n. This is a useful idea, for example, in the study of Diophantine equations: if such an equation has a solution in the integers, then it must have a solution modulo p^n for all n: to prove it does not have a solution, therefore, it suffices to show that it does not have a solution in $\mathbb{Z}_p$ for some prime p.

We can express the expansion of elements in $\mathbb{Z}_p$ as

$$\begin{aligned}\mathbb{Z}_p &= \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \\ &= \left\{ (\gamma_n)_{n=0}^{\infty} \in \textstyle\prod_{n \geq 0} \mathbb{Z}/p^n\mathbb{Z} : \text{for all } n, \gamma_{n+1} \equiv \gamma_n \pmod{p^n} \right\},\end{aligned}$$

which we will see is an example of a *projective limit.* That is, for each n we have a compatible system of maps

$$\begin{aligned}\mathbb{Z}_p &\to \mathbb{Z}/p^n\mathbb{Z} \\ \gamma &\mapsto c_0 + \cdots + c_{n-1}p^{n-1} = \gamma_n.\end{aligned}$$

In this way, $\mathbb{Z}_p$ is given the structure of a *profinite ring.* We can also take the unit group $\mathbb{Z}_p^* \subset \mathbb{Z}_p$, an example of a *profinite group*; as groups we have

$$\mathbb{Z}_p^* \cong \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p, & p > 2; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2, & p = 2. \end{cases}$$

Note that in fact these isomorphisms are not just algebraic but also respect the topology which underlies these objects.

2. Definitions and Examples

We now begin with the formal definitions. A *topological group* is a group G which is also a topological space with the property that the multiplication map

$$\begin{aligned} m : G \times G &\to G \\ (a, b) &\mapsto ab \end{aligned}$$

and the inversion map

$$\begin{aligned} i : G &\to G \\ a &\mapsto a^{-1} \end{aligned}$$

are continuous. Whenever we are given two topological groups, we insist that a homomorphism between them be continuous. In particular, an isomorphism between two topological groups must be an isomorphism of groups which is simultaneously an 'isomorphism' of their topological spaces, i.e. a homeomorphism.

A *directed partially ordered set* is a set I together with a partial order $\geq$ such that for any two elements $i, j \in I$, there exists a $k \in I$ such that $k \geq i$ and $k \geq j$. For example, we may take I to be the set of integers $\mathbb{Z}$ under the relation $n \geq m$ if $m \mid n$: for any $m_1, m_2 \in \mathbb{Z}$, we see that $\mathrm{lcm}(m_1, m_2) \geq m_1, m_2$.

A *projective system* is a collection of groups G_i (for $i \in I$) together with group homomorphisms $f_i^j : G_j \to G_i$ for $i, j \in I$ with $j \geq i$, such that $f_i^i = \mathrm{id}_{G_i}$ for every $i \in I$ and $f_i^j \circ f_j^k = f_i^k$ for $k \geq j \geq i$. Given any such projective system, one has a *projective limit*

$$\varprojlim_i G_i = \left\{ (\gamma_i)_{i \in I} \in \textstyle\prod_{i \in I} G_i : \text{for all } i, j \in I \text{ such that } j \geq i,\ f_i^j(\gamma_j) = \gamma_i \right\}.$$

This is not only a group, but a topological group as well: we give each G_i the discrete topology, the product the product topology, and the projective limit the restriction topology.

We define a *profinite group* to be a topological group which is isomorphic (as a topological group) to a projective limit of finite groups. One defines a *topological ring* and *profinite ring* similarly.

Example 2.1. *We define for any $g \in \mathbb{Z}$, $g \geq 1$, the projective limit*

$$\mathbb{Z}_g = \varprojlim_n \mathbb{Z}/g^n\mathbb{Z}.$$

As an exercise, one can see that as topological rings,

$$\mathbb{Z}_g \cong \prod_{p \mid g} \mathbb{Z}_p;$$

for example, the ring of 8-adic integers is isomorphic to the ring of 2-adic integers.

Example 2.2. *We also define the ring* $\widehat{\mathbb{Z}}$*, read* $\mathbb{Z}$-hat*. Here, we take the projective limit not over all powers of a given number, but over all numbers:*

$$\begin{aligned}\widehat{\mathbb{Z}} &= \varprojlim_n \mathbb{Z}/n\mathbb{Z} \\ &= \left\{(a_n)_{n=1}^{\infty} \in \textstyle\prod_{n=1}^{\infty}(\mathbb{Z}/n\mathbb{Z}) : \textit{for all } n \mid m, a_m \equiv a_n \pmod{n}\right\}.\end{aligned}$$

We give each $\mathbb{Z}/n\mathbb{Z}$ *the discrete topology, and* $\prod_n(\mathbb{Z}/n\mathbb{Z})$ *the product topology. This product is compact, as a result of the theorem of Tychonoff (the product of compact topological spaces is itself compact); the restriction* $\widehat{\mathbb{Z}}$ *is therefore itself compact, as* $\widehat{\mathbb{Z}}$ *is closed in* $\prod_n(\mathbb{Z}/n\mathbb{Z})$*. The ring homomorphism* $\mathbb{Z} \to \prod_n(\mathbb{Z}/n\mathbb{Z})$ *which takes every element to its reduction modulo n realizes* $\widehat{\mathbb{Z}}$ *as the closure of* $\mathbb{Z}$ *in the product* $\prod_n(\mathbb{Z}/n\mathbb{Z})$*.*

The relation of divisibility is a partial order: to replace this with a linear order, we may also represent this ring as

$$\widehat{\mathbb{Z}} \cong \{(b_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} \mathbb{Z}/n!\mathbb{Z} : \textit{for all } n, b_{n+1} \equiv b_n \pmod{n!}\}.$$

Here we write every element as

$$\gamma = c_1 + c_2 2! + c_3 3! + \cdots \in \widehat{\mathbb{Z}}$$

where we have digits $0 \leq c_i \leq i$*.*

It is also true that

$$\widehat{\mathbb{Z}} \cong \prod_{p \textit{ prime}} \mathbb{Z}_p.$$

After a bit of topological algebra, we see that one can also characterize profinite groups as follows: if G is a topological group, then G is profinite if and only if G is:

(a) Hausdorff,
(b) compact, and
(c) *totally disconnected*, i.e. that the largest connected subsets consist of single points, or what is the same, for any two points $x, y \in G$, there exists a set U which is both open and closed in G and which contains x but not y.

It is easy to see that each of our examples above is Hausdorff, compact because it is a closed subgroup of the compact product, and totally disconnected.

Given any G_i profinite, for i in a index set I, the product $\prod_i G_i$ is itself profinite; the product

$$\prod_{i \in I} \mathbb{Z}/2\mathbb{Z}$$

is an example of such a profinite group. Moreover, if G is a profinite group and $H \subset G$ is a closed subgroup, then H is profinite. Similarly, if $N \subset G$ is a closed normal subgroup, then G/N is profinite with the quotient topology.

It is a theorem that given a homomorphism of profinite groups $f : G_1 \to G_2$ (in particular, continuous), then $\ker f$ is a closed normal subgroup of G_1, so one may form the quotient $G_1/\ker f$; the image $f(G_1)$ is a closed subgroup of G_2, and in fact

$$G_1/\ker f \cong f(G_1)$$

as topological groups.

3. Galois Groups

In number theory, we have another source of profinite groups coming from Galois groups. Given an extension of fields $K \subset L$, the following are equivalent:

(a) $L = \bigcup_{\substack{K\subset M\subset L \\ M/K \text{finite, Galois}}} M$;
(b) $L \supset K$ is algebraic, normal, and separable;
(c) There is an algebraic closure $\overline{K}$ of K, and a subset $S \subset K[X]$ of monic polynomials such that for all $f \in S$, $\gcd(f, f') = 1$ (the polynomials are separable), and

$$L = K(\alpha \in \overline{K} : f(\alpha) = 0 \text{ for some } f \in S).$$

If one of these three equivalent properties holds, we say that L is *Galois* over K.

If $L \supset K$ is Galois, we have the *Galois group*

$$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}\, L : \sigma|_K = \mathrm{id}_K\}.$$

If $E \supset K$ is a finite extension such that $L \supset E$, and $\sigma \in \mathrm{Gal}(L/K)$, then the E-th neighborhood of σ, denoted $U_E(\sigma) = \{\tau : \tau|_E = \sigma|_E\}$, is by definition open; by ranging over E, we obtain an open system of neighborhoods of σ, which gives a topology on $\mathrm{Gal}(L/K)$. In this topology, two automorphisms are 'close' to one another if they agree on a large subfield.

To see that $\mathrm{Gal}(L/K)$ is a profinite group, we note that

$$\mathrm{Gal}(L/K) = \varprojlim_{M/K \text{ finite, Galois}} \mathrm{Gal}(M/K)$$

where now each $\mathrm{Gal}(M/K)$ is a finite group. The set of such M is a partially ordered set by inclusion. We may take the composed field of two subfields, which is again finite, so this set is directed. For $M \supset M'$ we have restriction maps $\mathrm{Gal}(M/K) \to \mathrm{Gal}(M'/K)$, so we have a projective system.

Many theorems of Galois theory readily generalize to this setting. For instance, we have an inclusion-reversing bijective correspondence

$$\begin{array}{ccc} \{E : K \subset E \subset L\} & \longleftrightarrow & \{H \subset \mathrm{Gal}(L/K) : H \text{ a closed subgroup}\} \\ E & \longmapsto & \mathrm{Gal}(L/E) = \mathrm{Aut}_E\, L \\ L^H & \longleftarrow\!\shortmid & H. \end{array}$$

Note that now we must insist in this correspondence that the subgroups be closed. Furthermore, if $H' \supset H$ are two closed subgroups such that $[H' : H] < \infty$, then as in the case of finite Galois theory we have $[L^H : L^{H'}] = [H' : H]$.

Now let $\overline{K}$ be an algebraic closure of K. Consider the *separable closure of* K, $\overline{K} \supset K^{\text{sep}} \supset K$, namely,

$$K^{\text{sep}} = \{\alpha \in \overline{K} : \alpha \text{ separable over } K\}.$$

The *absolute Galois group* G_K of K is the defined to be $\mathrm{Gal}(K^{\text{sep}}/K)$. We treat G_K as a fundamental object of study because it allows us to control all separable extensions L of K in one stroke. Indeed, some might say that number theory is the study of $G_{\mathbb{Q}}$.

One also has the maximal abelian extension $K^{\text{ab}} \supset K$, the composite of all field extensions of K with an abelian Galois group. This is a Galois extension with $\mathrm{Gal}(K^{\text{ab}}/K)$ an abelian profinite group: i.e.

$$\mathrm{Gal}(K^{\text{ab}}/K) \cong G_K/[G_K, G_K].$$

Here, the quotient is by the closure of the (usual algebraic) commutator subgroup of G_K, the smallest subgroup which gives an abelian quotient. This is sometimes called the *abelianized Galois group* G_K^{ab}.

Example 3.1. *For the rational numbers $\mathbb{Q}$, we have that*

$$G_{\mathbb{Q}}^{\text{ab}} \cong \widehat{\mathbb{Z}}^* \cong \prod_{p \text{ prime}} \mathbb{Z}_p^*.$$

It is a theorem of Kronecker-Weber that the maximal abelian extension of $\mathbb{Q}$ is $\mathbb{Q}^{\text{ab}} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. The isomorphism above arises from the isomorphism

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^* &\cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ a \bmod n &\mapsto (\zeta_n \mapsto \zeta_n^a) \end{aligned}$$

Example 3.2. *If K is a finite field, then $G_K \cong \widehat{\mathbb{Z}}$.*

Exercises

Exercise 1.1. Let p be a prime number. Prove that there is a map $\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ that is simultaneously an isomorphism of rings and a homeomorphism of topological spaces.

Exercise 1.2. Prove that any continuous bijection from one profinite group to another is a homeomorphism.

Exercise 1.3.

(a) Let g be an integer, $g > 1$, and define $\mathbb{Z}_g = \varprojlim \mathbb{Z}/g^n\mathbb{Z}$. Prove that $\mathbb{Z}_g$ is, as a profinite group, isomorphic to $\prod_{p|g} \mathbb{Z}_p$, the product ranging over the primes p dividing g.

(b) Define $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$, the limit ranging over the set of positive integers n, ordered by divisibility. Prove: $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$, the product ranging over all primes p.

Exercise 1.4.

(a) Prove that each $a \in \widehat{\mathbb{Z}}$ has a unique representation as $a = \sum_{n=1}^{\infty} c_n n!$, with $c_n \in \mathbb{Z}$, $0 \le c_n \le n$.

(b) Let b be a non-negative integer, and define the sequence $(a_n)_{n=0}^{\infty}$ of non-negative integers by $a_0 = b$ and $a_{n+1} = 2^{a_n}$. Prove that $(a_n)_{n=0}^{\infty}$ converges in $\widehat{\mathbb{Z}}$, and that the limit is independent of the choice of b.

(c) Let $a = \lim_{n\to\infty} a_n \in \widehat{\mathbb{Z}}$ be as in (b), and write $a = \sum_{n=1}^{\infty} c_n n!$ as in (a). Determine c_n for $1 \le n \le 10$.

Exercise 1.5. Let G and H be profinite groups, and let $f\colon G \to H$ be a continuous group homomorphism. Prove that $\ker f$ is a closed normal subgroup of G, that $f(G)$ is a closed subgroup of H, and that f induces an isomorphism $G/\ker f \xrightarrow{\sim} f(G)$ of profinite groups; here $G/\ker f$ has the quotient topology induced by the topology on G, and $f(G)$ has the relative topology induced by the topology on H.

Exercise 1.6. The *profinite completion* of a group G is the profinite group $\widehat{G}$ defined by $\widehat{G} = \varprojlim G/N$, with N ranging over the set of normal subgroups of G of finite index, ordered by containment, the transition maps being the natural ones.

(a) Prove that there is a natural group homomorphism $G \to \widehat{G}$, and that its image is dense in $\widehat{G}$. Find a group G for which f is not injective.

(b) What is the profinite completion of the additive group of $\mathbb{Z}$?

Exercise 1.7. Let p be a prime number.

(a) Show that there is a group G whose profinite completion is isomorphic to the additive group $\mathbb{Z}_p$. Can you find such a G that is countable?

(b) Let A be the product of a countably infinite collection of copies of $\mathbb{Z}/p\mathbb{Z}$. Is there a group G such that A is isomorphic to the profinite completion of G? Prove the correctness of your answer.

Exercise 1.8. Prove: $\widehat{\mathbb{Z}}^* \cong \widehat{\mathbb{Z}} \times \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$ as profinite groups.

Exercise 1.9.

(a) Prove: for every positive integer n the natural map $\mathbb{Z}/n\mathbb{Z} \to \widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}}$ is an isomorphism.

(b) Prove that there is a bijection from the set of positive integers to the set of open subgroups of $\widehat{\mathbb{Z}}$ mapping n to $n\widehat{\mathbb{Z}}$.

(c) Can you classify all closed subgroups of $\widehat{\mathbb{Z}}$?

Exercise 1.10. Let p be a prime number, and view $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ as a closed subgroup of the profinite group $A = \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$. Prove that A and $\mathbb{Z}_p \times (A/\mathbb{Z}_p)$ are isomorphic as groups but not as profinite groups.

Exercise 1.11. Let L be the field obtained from $\mathbb{Q}$ by adjoining all $a \in \mathbb{C}$ with $a^2 \in \mathbb{Q}$ to $\mathbb{Q}$. Prove: L is Galois over $\mathbb{Q}$, and $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to the product of a countably infinite number of copies of $\mathbb{Z}/2\mathbb{Z}$.

Exercise 1.12. Let K be a field, with separable closure K^{sep}, and let K^{ab} be the maximal abelian extension of K inside K^{sep}. Write $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Prove that K^{ab} is a Galois extension of K, and that $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is isomorphic to $G_K/[G_K, G_K]$, where $[G_K, G_K]$ denotes the closure of the commutator subgroup of G_K.

Exercise 1.13. Let L be a field, and view $\mathrm{Aut}\, L$ as a subset of the set $L^L = \prod_{x \in L} L$ of all functions $L \to L$. Give L the discrete topology, L^L the product topology, and $\mathrm{Aut}\, L$ the relative topology.

(a) Prove: $\mathrm{Aut}\, L$ is a topological group; i. e., the composition map $\mathrm{Aut}\, L \times \mathrm{Aut}\, L \to \mathrm{Aut}\, L$ and the map $\mathrm{Aut}\, L \to \mathrm{Aut}\, L$ sending each automorphism of L to its inverse are continuous.

(b) Let K be a subfield of L. Prove: L is Galois over K if and only if there is a compact subgroup G of $\mathrm{Aut}\, L$ such that K is the field of invariants of G. Prove also that such a subgroup G, if it exists, is necessarily equal to $\mathrm{Gal}(L/K)$, and that its topology coincides with the Krull topology on $\mathrm{Gal}(L/K)$. (The Krull topology is the topology of $\mathrm{Gal}(L/K)$ when viewed as a profinite group.)

Mathematisch Instituut,
Universiteit Leiden,
Postbus 9512,
2300 RA Leiden,
The Netherlands
E-mail address: `hwl@math.leidenuniv.nl`