Profinite Groups

Navid Rashidian

1 Category Theory

Definition 1.1. A *category* $\mathcal{C}$ consists of collections $\mathrm{Obj}(\mathcal{C})$ and $\mathrm{Mor}(\mathcal{C})$, respectively called the objects and morphisms of $\mathcal{C}$ such that

- there are functions $s\colon \mathrm{Mor}(\mathcal{C}) \to \mathrm{Obj}(\mathcal{C})$ and $t\colon \mathrm{Mor}(\mathcal{C}) \to \mathrm{Obj}(\mathcal{C})$ assigning to each morphism a source and a target;
- for each object $X \in \mathrm{Obj}(\mathcal{C})$ there is a distinguished morphism $\mathrm{id}_X \in \mathrm{Mor}(\mathcal{C})$ such that $s(\mathrm{id}_X) = t(\mathrm{id}_X) = X$; and
- for each pair of morphisms f, g such that $t(f) = s(f)$ there is a morphism $g \circ f$ with $s(g \circ f) = s(f)$ and $t(g \circ f) = t(g)$ called their composition;

satisfying the further conditions that $(f \circ g) \circ h = f \circ (g \circ h)$ and $\mathrm{id}_X \circ f = f$ and $f \circ \mathrm{id}_X = f$ wherever these expressions make sense.

Remark 1.2. We write $f\colon X \to Y$ to denote a morphism $f \in \mathrm{Mor}(\mathcal{C})$ with $s(f) = X$ and $t(f) = Y$.

Definition 1.3. Let $\mathcal{C}$ be a category. If both $\mathrm{Obj}(\mathcal{C})$ and $\mathrm{Mor}(\mathcal{C})$ are sets, The category $\mathcal{C}$ is called a *small category*. $\mathcal{C}$ is called *locally small* if for every objects $X, Y \in \mathrm{Obj}(\mathcal{C})$ the collection of morphisms $f \in \mathrm{Mor}(\mathcal{C})$ with $s(f) = X$ and $t(f) = Y$ is a set. In a locally small category for objects $X, Y \in \mathrm{Obj}(\mathcal{C})$ we define the *hom-set of* X *and* Y as

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) = \{f \in \mathrm{Mor}(\mathcal{C}) : s(f) = X \text{ and } t(f) = Y\}$$

Definition 1.4. Let $\mathcal{C}$ be a category and $f\colon X \to Y$ a morphism in $\mathcal{C}$. We call f an *isomorphism* if there is a morphism $g\colon Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. If such morphisms exist, we call X and Y *isomorphic*.

Definition 1.5. Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A *(covariant) functor* $F\colon \mathcal{C} \to \mathcal{D}$ consists of maps $\mathrm{Obj}(\mathcal{C}) \to \mathrm{Obj}(\mathcal{D})$ and $\mathrm{Mor}(\mathcal{C}) \to \mathrm{Mor}(\mathcal{D})$ such that

- for every $f \in \mathrm{Mor}(\mathcal{C})$ we have $s(F(f)) = F(s(f))$ and $t(F(f)) = F(t(f))$;
- for every $X \in \mathrm{Obj}(\mathcal{C})$ we have $F(\mathrm{id}_X) = \mathrm{id}_F(X)$; and
- for every pair of morphisms $f, g \in \mathrm{Mor}(\mathcal{C})$ with a defined composition $F(g \circ f) = F(g) \circ F(f)$.

Definition 1.6. Suppose $\mathcal{C}$ is a category. The *opposite category* denoted by $\mathcal{C}^{\mathrm{op}}$ is the category with the same objects and morphisms as $\mathcal{C}$ such that $s_{\mathcal{C}^{\mathrm{op}}}(f) = t_{\mathcal{C}}(f)$ and $t_{\mathcal{C}^{\mathrm{op}}}(f) = s_{\mathcal{C}}(f)$ and $g \circ_{\mathcal{C}^{\mathrm{op}}} f = f \circ_{\mathcal{C}} g$.

Definition 1.7. A *contravariant function* $F\colon \mathcal{C} \to \mathcal{D}$ is a covariant functor $F\colon \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$.

Example 1.8. A *preorder* is a small categoy $\mathcal{P}$ such that for every objects $X, Y \in \mathrm{Obj}(\mathcal{P})$ we have $\#\mathrm{Hom}_{\mathcal{P}}(X, Y) \leq 1$. If for every $X, Y \in \mathrm{Obj}(\mathcal{P})$ there is an object $Z \in \mathrm{Obj}(\mathcal{P})$ with morphisms $f\colon X \to Z$ and $g\colon Y \to Z$, the preorder $\mathcal{P}$ is called a *directed set*. For $I, J \in \mathrm{Obj}(\mathcal{P})$ we write $I \leq J$ if $\#\mathrm{Hom}_{\mathcal{P}}(X, Y) = 1$.

Example 1.9. A *partially ordered set (poset)* is a small categoy $\mathcal{P}$ such that for every pair of objects $X, Y \in \mathrm{Obj}(\mathcal{P})$ we have

$$\#\big(\mathrm{Hom}_{\mathcal{P}}(X, Y) \cup \mathrm{Hom}_{\mathcal{P}}(Y, X)\big) \leq 1$$

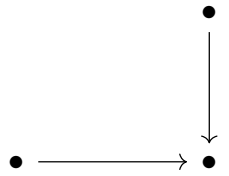
. For posets $\mathcal{P}_1$ and $\mathcal{P}_2$ an order-preserving (-reversing) function from $\mathcal{P}_1$ to $\mathcal{P}_2$ is exactly a covariant (contravariant) functor $F\colon \mathcal{P}_1 \to \mathcal{P}_2$.

Example 1.10. Sets and functions constitute a category denoted by **Set**. Groups and group homomorphisms constitute a category denoted by **Grp**. Topological spaces and continuous functions constitute a category denoted by **Top**. Topological groups and continuous homomorphisms constitute a category denoted by **TopGrp**. All of these categories are locally small but none is small.

Example 1.11. The category **2** is the category consisting of two objects and only the required identity morphisms:

A funtor $F\colon \mathbf{2} \to \mathcal{C}$ is just a pair of objects from $\mathrm{Obj}(\mathcal{C})$. Similarly, for every cardinality κ we can define a discrete category with cardinality κ to serve as an index set.

Example 1.12. The following diagram describes a category consisting of three objects and two morphisms (in addition to the required identity morphisms):



Call this category $\mathcal{J}$. A functor $F\colon \mathcal{J} \to \mathcal{C}$ describes a diagram of the following shape in the category $\mathcal{C}$:

$$\begin{array}{ccc} & & X \\ & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow{g} & Z \end{array}$$

This justifies us calling a functor from a small category a diagram.

Definition 1.13. Let $F\colon \mathcal{J} \to \mathcal{C}$ be a diagram. A *cone* over F is a an object $X \in \mathrm{Obj}(\mathcal{C})$ and a collection of morphisms $\alpha_J\colon X \to F(J)$ indexed by objects $J \in \mathrm{Obj}(\mathcal{J})$ such that for every morphism $f\colon J \to J'$ we have $F(f) \circ \alpha_J = \alpha_{J'}$.

Example 1.14. A diagram $F\colon \mathbf{2} \to \mathcal{C}$ is just a pair of discrete objects $X, Y \in \mathrm{Obj}(\mathcal{C})$. A cone over F is just an object $A \in \mathrm{Obj}(\mathcal{C})$ and a pair of morphisms $f\colon A \to X$ and $g\colon A \to Y$.

Example 1.15. Recall the category $\mathcal{J}$ from example 1.12. A cone over $F : \mathcal{J} \to \mathcal{C}$ is fully described by an object $A \in \mathrm{Obj}(\mathcal{C})$ and morphisms $\alpha\colon A \to X$ and $\beta\colon A \to Y$ such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & X \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow{g} & Z \end{array}$$

(Note that we don't need to explicitly describe the morphism $A \to Z$ included in the cone.)

Definition 1.16. Let $F\colon \mathcal{J} \to \mathcal{C}$ be a diagram. A *limit of* F is a cone $\langle L, \alpha_J \rangle$ over F such that for every cone $\langle N, \beta_J \rangle$ over F there is a unique morphism $u\colon N \to L$ such that for every $J \in \mathrm{Obj}(\mathcal{J})$ we have $\beta_J = \alpha_J \circ u$.

Remark 1.17. Let $\langle L, \alpha_J \rangle$ and $\langle L', \beta_J \rangle$ be limits of $F : \mathcal{J} \to \mathcal{C}$. By definition there are morphisms $u\colon L' \to L$ and $u'\colon L \to L'$ such that for every $J \in \mathrm{Obj}(\mathcal{J})$ we have $\beta_J = \alpha_J \circ u$ and $\alpha_J = \beta_J \circ u'$. It follows that for every $J \in \mathrm{Obj}(\mathcal{J})$ we have $\alpha_J = \alpha_J \circ (u \circ u')$. According to the definition of limit only one function should play such role, so $u \circ u' = \mathrm{id}_L$ and similarly $u' \circ u = \mathrm{id}_{L'}$. Therefore L and L' are isomorphic. As a folk who have internalized Leibniz's principle of the Identity of Indiscernibles, this makes us usually talk about *the* limit of a diagram.

Example 1.18. Consider a diagram $F\colon \mathbf{2} \to \mathbf{Set}$ consisting of sets X and Y. It is easy to verify that the cartesian product $X \times Y$ with the obvious projection maps π_X and π_Y is a limit of F. The same is true if we replace $\mathbf{2}$ with another discrete category with the requisite cardinality serving as an index set.

Example 1.19. Let $\mathcal{I}$ be a discrete category serving us an index set. A functor $F\colon \mathcal{I} \to \mathbf{Top}$ is a family $\big\langle \langle X_I, \tau_I \rangle \big\rangle$ of toplogical spaces indexed by $\mathcal{I}$. Let $X = \langle \prod X_I, \tau \rangle$ and the obvious projection mappings π_{X_I} the cartesian product of the X_I's with the usual product topology having the collection of all $(\pi_{X_I})^{-1}(U)$'s for some $U \in \tau_I$ as a subbasis. Since continuous maps are set maps it is obvious that for any given cone $\langle Y, \alpha_{X_I} \rangle$ there is only one possible candidate defined by $u\colon y \mapsto (\alpha_{X_I}(y))$ as the required morphism $Y \to X$. Hence, we only need to show that u is continuous if the α_{X_I}'s are. This last fact is obvious since every elements of the subbasis according to which τ is defined is in the form of $(\pi_{X_I})^{-1}(U)$ and $u^{-1}((\pi_{X_I})^{-1}(U)) = (\alpha_I)^{-1}(U)$ which is gauranteed to be open if α_I is continuous.

If we instead equip $\prod X_I$ with the box topology generated by sets in the form of $\prod U_I$ such that every U_I is a member of τ_I, the map $y \mapsto (\alpha_{X_I}(y))$ will not be necessarily continuous. Moreover the cartesian product of compact topological spaces equipped with the box topology is not necessarily compact, while their cartesian product equipped with the product topology is necessarily so. (See Wikipedia: Box Topology.)

2 Projective Systems and Projective Limits

Definition 2.1. Let $\mathcal{I}$ be a preordered set. A contravariant functor $F\colon \mathcal{I} \to \mathcal{C}$ is called a *projective* (or *inverse*) *system*.

Remark 2.2. Since in a preorder there is at most one morphism between any two objects, in a given projective system we could denote the possible morphism $X_J \to X_I$ as φ_{IJ} without ambiquity (note the difference in order). We will usually denote a projective system by $\langle X_I, \varphi_{IJ}\rangle$. We will also usually call describe the family of maps in a cone on F as a family of maps compatible with the projective system.

Definition 2.3. Let $F\colon \mathcal{I} \to \mathcal{C}$ be a projective system. The limit of F is called the *projective limit* or *inverse limit* of this system and is denoted by $\varprojlim X_I$.

Example 2.4. In the category **Set** for a given projective system $\langle X_I, \varphi_{IJ}\rangle$ the following explicit construction equipped with the obvious projection maps π_I describes a projective limit:

$$\varprojlim X_I = \{(x_I) \in \prod X_I : \varphi_{IJ}(x_J) = x_I \text{ for every } I, J \in \mathrm{Obj}(\mathcal{I})\}$$

For a family of maps $\varphi_I\colon Y \to X_I$ compatible with the projective system, the map $x \mapsto (\varphi_I(x))$ is clearly the unique map $H \to \varprojlim X_I$ described in the definition of limit. The fac that $(\varphi_I(x))$ falls inside $\varprojlim X_I$ is gauranteed by the compatibility of the set of maps with the projective system.

Example 2.5. Consider the following projective system in **Set**:

$$\begin{array}{ccc} & & \{0\} \\ & & \big\downarrow \\ \{1\} & \hookrightarrow & \{0,1\} \end{array}$$

This projective system is modelled on a preordered set that is not directed. It is easy to verify that its limit is empty.

Example 2.6. Let $\langle G_I, \varphi_{IJ}\rangle$ be a projective system in the category **Grp**. Let

$$G = \{(x_I) \in \prod G_I : \varphi_{IJ}(x_J) = x_I \text{ for every } I, J \in \mathrm{Obj}(\mathcal{I})\}$$

and π_I's the obvious projection maps. The identity element of $\prod G_I$ is clearly in G and hence G is necessarily non-empty. Also it is easy to verify that G is a group. Finally, for every group H and set of morphisms $\psi_I \colon H \to G_I$ we have, the map $u \colon H \to G$ defined by $x \mapsto (\psi_I(x))$ is the sole group homomorphism satisfying the desired property in the definition of projective limits. Hence, $\varprojlim G_I = G$.

We saw in Example 2.5 that the projective limit of a projective system need not be non-empty. The following theorem gives us sufficient conditions for having a non-empty projective limit of finite sets:

Proposition 2.7. *Let $\mathcal{I}$ be a directed set and $\langle X_i, \varphi_{IJ} \rangle$ a projective system modelled on $\mathcal{I}$. Let $X = \varprojlim X_I$. Then*

(i) If all X_I's are non-empty, then X is non-empty.

(ii) For each $I \in \mathrm{Obj}(\mathcal{I})$ we have

$$\pi_I(X) = \bigcap_{I \leq J} \varphi_{IJ}(X_J)$$

Proof. See [1, Proposition 1-11]. □

3 Profinite Groups

Definition 3.1. A topological group G is called a *profinite group* if there is a projective system $\langle G_I, \varphi_{IJ} \rangle$ such that G is the projective limit of this projective system in the category **TopGrp**. The topology on G is called the *profinite topology.*

Proposition 3.2. *Let G be a profinite group, given as a limit of the projective system $\langle G_I, \varphi_{IJ} \rangle$. Then,*

(a) G is Hausdorff;

(b) G is a closed subset of the direct product $\prod G_I$; and

(c) G is compact.

Proof. (a) The direct product of Hausdorff spaces is Hausdorff. Hence, G is Hausdorff.

(b)

(c) The direct product $\prod G_I$ is compact. A closed subset of a compact space equipped with the subspace topology is compact.

□

3.1 p-adic Numbers

Definition 3.3. Let R be an integral domain. An *absolute value on* R is a function $|.|\colon R \to \mathbb{R}$ such that for every $x, y \in R$ we have

(a) $|x| \geq 0$;

(b) $|x| = 0$ iff $x = 0$;

(c) $|xy| = |x||y|$; and

(d) $|x + y| \leq |x| + |y|$.

Definition 3.4. A *metric space* is a set M equipped with a function $d\colon M \times M \to \mathbb{R}$ such that for every $x, y, z \in M$ we have

(a) $d(x, x) = 0$;

(b) if $x \neq y$ then $d(x, y) > 0$;

(c) $d(x, y) = d(y, x)$; and

(d) $d(x, z) \leq d(x, y) + d(y, z)$.

Proposition 3.5. *Let R be an integral domain and $|.|$ an absolute value defined on R. Then $d(x, y) = |x - y|$ is a metric on R.*

Definition 3.6. For any point $x \in M$ and any real number $r > 0$ *the open ball of radius r around x* is defined by

$$B_r(x) = \{y \in M : d(x, y) < r\}$$

The open balls form the basis for the *metric topology on M*.

Definition 3.7. A sequence (x_n) of points in a metric space M is a *Cauchy sequence* if for every $r > 0$ there is a positive integer N such that for every pair of positive integers $m, n \geq N$ we have $d(m, n) < r$. Two Cauchy sequences (x_n) and (y_n) are called *equivalent* if $x_n - y_n$ converges to zero.

Proposition 3.8. *(a) The equivalence defined on Cauchy sequences is an equivalence relation.*

(b) Sum of two Cauchy sequences is Cauchy.

(c) Suppose $(x_i) \sim (y_i)$ *and* $(x_i') \sim (y_i')$. *Then* $(x_i + x_i') \sim (y_i + y_i')$.

Definition 3.9. A *complete metric space* is a metric space in which every Cauchy sequence converges to a point in the space.

Definition 3.10. Let p be a fixed prime. The *p-adic valuation* is the function $v_p \colon \mathbb{Z} \to \mathbb{Z}^+ \cup \{\infty\}$ which assigns to each positive integer n the unique e such that $n = p^e m$ and $p \nmid m$ and assigns ∞ to 0. The *p-adic absolute value* is the function $|.|_p \colon \mathbb{Z} \to \mathbb{R}$ defined by $|n|_p = p^{-v_p(n)}$.

Proposition 3.11. *The p-adic absolute value is an absolute value on* $\mathbb{Z}$.

Example 3.12. Integers are not complete under the p-adic metric. The sequence $(p^n + 1)$ is clearly Cauchy but doesn't converge to any integer.

Definition 3.13. The group $\mathbb{Z}_p$ called the group of *p-adic integers* is the completion of $\mathbb{Z}$ with respect to the p-adic metric.

We now want to prove that $\mathbb{Z}_p$ defined as the completion of $\mathbb{Z}$ with respect to the p-adic metric is the inverse limit of the projective system $\mathbb{Z}/p^e\mathbb{Z}$ with the natural projections $\varphi_{n(n+1)} \colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$.

Proposition 3.14. *The following are equivalent:*

(a) $|x_n - x_m|_p \leq p^{-e}$.

(b) $v_p(x_n - x_m) \geq e$.

(c) $x_n \equiv x_m \mod p^e$.

Proof. Expand the definitions. □

Proposition 3.15. *Consider* $\mathbb{Z}$ *with the metric induced by the p-adic absolute value for a fixed prime p. Let* (x_n) *be a Cauchy sequence. For every positive integer e the remainder of* x_i*'s modulo* p^e *eventually stops. Moroever, if* (x_n) *and* (y_n) *are equivalent Cauchy sequences, their remainders modulo* p^e *stop on the same number. Therefore, remainder modulo* p^e *defines a function* $\varphi_e \colon \mathbb{Z}_p \to \mathbb{Z}/p^e\mathbb{Z}$. *The function* φ_e *is a continuous group homomorphism.*

Proof. Let $r = p^{-e}$. There is a positive integer N such that for every pair of positive integers $m, n > N$ we have $x_m - x_n < r$ or equivalently

$$x_m \equiv x_n \mod p^e$$

A similar argument proves the other claim. That φ_e respects addition is obvious. For continuity note that if $\varphi_e((x_n)) = \varphi_e((y_n))$ then □

3.2 Profinite integers

References

[1] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier Analysis on Number Fields*. Graduate Texts in Mathematics 186. New York: Springer, 1999. ISBN: 978-0-387-98436-0.