Universidad del País Vasco Euskal Herriko Unibertsitatea

ZTF-FCT
Zientzia eta Teknologia Fakultatea
Facultad de Ciencia y Tecnología

Advanced Course in Algebra and Topology 2016

Course notes

Igor Arrieta Torres
Leire González Cincunegui
José Miguel Ibarreche Olea
Andoni Zozaya Ursuegi

Leioa, Summer 2016

We would like to express our gratitude to all the people who have contributed to write and to edit these notes. In particular to Gustavo A. Fernández Alcober, F. Javier Gutiérrez García, Jon González Sánchez and Iraide Mardones Pérez.

Contents

Part I

Topology

Chapter 1

Product topologies

1.1 Arbitrary products

1.1.1 Finite product

Let X_1 and X_2 be two sets. The *cartesian product* is defined as

$$X_1 \times X_2 = \{(x_1, x_2) \mid x_1 \in X_1,\ x_2 \in X_2\}$$

where the next two properties are satisfied:

First of all, there exist the projections

$$\pi_i \colon X_1 \times X_2 \to X_i$$

with $i \in \{1, 2\}$.

Secondly, a universal property is satisfied, that is, given a set Y and two maps $f_i : Y \to X_i$, $i = 1, 2$, then there exists a unique map $F \colon Y \to X_1 \times X_2$ that makes the next diagram commutative:

$$\begin{tikzcd} X_1 \times X_2 \arrow[r, "\pi_i"] & X_i \\ Y \arrow[u, "F"] \arrow[ur, "f_i"'] & \end{tikzcd}$$

The diagram being commutative means that the only way to define F is as follows: given $y \in Y$, then $F(y) = (f_1(y), f_2(y))$.

1.1.2 Countably infinite product

In a similar way to the finite case, given a family of sets $\{X_n\}_{n\in\mathbb{N}}$ the *cartesian product* is defined as

$$X = \prod_{n\in\mathbb{N}} X_n = \{(x_n)_{n\in\mathbb{N}} \mid x_n \in X_n,\ \forall n \in \mathbb{N}\}$$

and as before we have the projections

$$\pi_n \colon X \to X_n$$

for all $n \in \mathbb{N}$, and the universal property that says that given a set Y and a collection of maps $(f_n \colon Y \to X_n)_{n\in\mathbb{N}}$, then there exists a unique map $F \colon Y \to X$ such that the following diagram is commutative:

$$\begin{tikzcd} X \arrow[r, "\pi_i"] & X_i \\ Y \arrow[u, "F"] \arrow[ur, "f_i"'] & \end{tikzcd}$$

In this way F is defined as $F(y) = (f_1(y), f_2(y), \dots)$ for each $y \in Y$.

1.1.3 Arbitrary infinite product

A pair of elements (x_1, x_2) can be understood as a map

$$\varphi \colon \{1,2\} \to X_1 \cup X_2$$

such that $\varphi(i) \in X_i$, $i = 1, 2$.
In a similar way, a sequence $(x_1, x_2, \dots)$ is a map

$$\varphi \colon \mathbb{N} \to \bigcup_{n\in\mathbb{N}} X_n$$

such that $\varphi(n) \in X_n$ for all $n \in \mathbb{N}$.
Taking this facts into consideration given a collection of sets $\{X_i\}_{i\in I}$, the cartesian product of $\{X_i\}_{i\in I}$ is defined as

$$X = \prod_{i\in I} X_i = \Big\{ \varphi \colon I \to \bigcup_{i\in I} X_i \mid \varphi(i) \in X_i,\ \forall i \in I \Big\}.$$

Sometimes we also write $X = \{\varphi(i)\}_{i\in I}$. As in the former cases the two properties are satisfied:

There exist the projections: for all $i \in I$, the ith projection is

$$\pi_i \colon X \to X_i$$

where $\pi_i(\varphi) = \varphi(i)$, for all $i \in I$.

The universal property is also satisfied: given a set Y and a collection of maps $(f_i \colon Y \to X_i)_{i\in I}$ there exists a unique map $F \colon Y \to X$ such that the next diagram is commutative:

$$\begin{tikzcd} X \arrow[r, "\pi_i"] & X_i \\ Y \arrow[u, "F"] \arrow[ur, "f_i"'] & \end{tikzcd}$$

For it being commutative F must be defined as $F(y)\colon I \to \bigcup_{i\in I} X_i$ where $F(y)(i) = f_i(y)$.

These two properties make the cartesian product be a product in the category of sets.

Remark. When we have a family of sets $\{X_i\}_{i\in I}$ such that $X_i = X$ for all $i \in I$, then the product is denoted X^I and it is called a cartesian power instead of cartesian product.

1.2 Product topology

Let (X_1, τ_1) and (X_2, τ_2) be two topological spaces. We consider the basis

$$\beta = \{U_1 \times U_2 \mid U_1 \in \tau_1,\ U_2 \in \tau_2\}$$

and the topology generated by this basis

$$\tau = \langle \beta \rangle.$$

We want $(X_1 \times X_2,\ \tau)$ be a product in the category of topological spaces. We are going to check that the two properties we have previously seen are verified. In this category we have to deal with continuous maps.

We have the projections

$$\pi_i\colon (X_1 \times X_2, \tau) \to (X_i, \tau_i)$$

where $i = 1, 2$. These projections are continuous: given $U_i \in \tau_i$, then $\pi_i^{-1}(U_i) = U_1 \times X_2 \in \beta \subseteq \tau$.

Now, the universal property is satisfied: given a set Y and two continuous maps $f_i\colon (Y, \tau_Y) \to (X_i, \tau_i)$, $i = 1, 2$, then there exists a unique map $F\colon (Y, \tau_Y) \to (X_1 \times X_2, \tau)$ that makes the following diagram commutative:

$$\begin{tikzcd}
(X, \tau) \arrow[r, "\pi_i"] & (X_i, \tau_i) \\
(Y, \tau_Y) \arrow[u, "F"] \arrow[ur, "f_i"'] &
\end{tikzcd}$$

The diagram being commutative means that the only way to define F is as follows: given $y \in Y$, then $F(y) = (f_1(y), f_2(y))$. Now we have to prove that F is continuous: given $U_1 \times U_2 \in \beta$, then $F^{-1}(U_1 \times U_2) = f_1^{-1}(U_1) \cap f_2^{-1}(U_2) \in \tau$.

1.2.1 Box topology

Let $\{(X_i, \tau_i)\}_{i\in I}$ be a family of topological spaces and consider

$$\beta = \left\{ \prod_{i\in I} U_i \mid U_i \in \tau_i,\ \forall i \in I \right\}.$$

Then β is the basis of the *box topology* τ_{Box}.

Sometimes it is considered a family of topologies $\{(X_i, \tau_i)\}_{i\in I}$ with β_i a basis of τ_i. It is easy to check that the family

$$\beta' = \left\{ \prod_{i\in I} U_i \mid U_i \in \beta_i, \forall i \in I \right\}$$

forms a basis of the box topology.

Remark. This topology is not called the product topology because it does not satisfy the universal property. However, we also have continuous projections: For all $i \in I$, it is defined $\pi_i \colon (X = \prod_{i\in I} X_i, \tau_{Box}) \to (X_i, \tau_i)$ such that $\pi_i(\varphi) = \varphi(i)$ and it is continuous: given $U_i \in \tau_i$, then $\pi_i^{-1}(U_i) \in \beta \subseteq \tau_{Box}$.

Now we are going to see an example where the universal property fails.

Example 1.2.1. Let us consider $(X_n, \tau_n) = (\mathbb{R}, \tau_u)$, for all $n \in \mathbb{N}$. Then $X = \prod_{n\in\mathbb{N}} X_n = \mathbb{R}^{\mathbb{N}}$. As we have seen a basis of this topology is:

$$\beta = \left\{ \prod_{n\in\mathbb{N}} (a_n, b_n) \mid (a_n, b_n) \in \beta_n,\ \forall n \in \mathbb{N} \right\}.$$

The universal property would say that for all (Y, τ_Y) and for all families $(f_n \colon (Y, \tau_Y) \to (\mathbb{R}, \tau_u))_{n\in\mathbb{N}}$ of continuous maps, there would exist a unique map $F \colon (Y, \tau_Y) \to (\mathbb{R}^{\mathbb{N}}, \tau)$ making the following diagram commutative:

$$\begin{tikzcd}
(\mathbb{R}^{\mathbb{N}}, \tau_{Box}) \arrow[r, "\pi_n"] & (\mathbb{R}, \tau_u) \\
(Y, \tau_Y) \arrow[u, "F"] \arrow[ur, "f_n"'] &
\end{tikzcd}$$

We are going to prove that this F does not exist always. Indeed, let $(Y, \tau_Y) = (\mathbb{R}, \tau_u)$ and consider for all $n \in \mathbb{N}$ the continuous map $f_n = 1_{\mathbb{R}} \colon (\mathbb{R}, \tau_u) \to (\mathbb{R}, \tau_u)$. In this case, the diagram being commutative would imply that F has to de defined as $F \colon (\mathbb{R}, \tau_u) \to (\mathbb{R}^{\mathbb{N}}, \tau_{Box})$ such that $F(x) = (x, x, x, \ldots)$ and this is not a continuous map: given $U = \prod_{n\in\mathbb{N}}(-\frac{1}{n}, \frac{1}{n}) \in \tau_{Box}$ then

$$F^{-1}(U) = \bigcap_{n\in\mathbb{N}} \left(-\tfrac{1}{n}, \tfrac{1}{n}\right) = \{0\} \notin \tau_u.$$

Remark. Note that this fails because the intersection of open sets is not necessarily open. If we consider the box topology of a finite family of topological spaces then this works, i.e. if I is finite then the topological space $(\prod_{i\in I} X_i, \tau_{Box})$ is the product of $\{(X_i, \tau_i)\}_{i\in I}$ in the category of topological spaces.

1.2.2 Product topology

Given a map $f \colon X \to (Y, \tau_y)$ we can search the coarsest topology on X that makes f continuous. This topology is called the *initial topology* on X. We can also do the same for a family of functions on X. The construction of the product topology is based on this idea.

Let $\{(X_i, \tau_i)\}_{i\in I}$ be a family of topological spaces. Given

$$\pi_i\colon X = \prod_{i\in I} X_i \to (X_i, \tau_i),$$

for all $i \in I$, we consider the collection

$$\sigma = \{\pi_i^{-1}(U_i) \mid i \in I,\ U_i \in \tau_i\}.$$

This is a subbasis of some topology, and the topology generated (as subbasis) by it,

$$\tau_{Tych} = \langle \sigma \rangle,$$

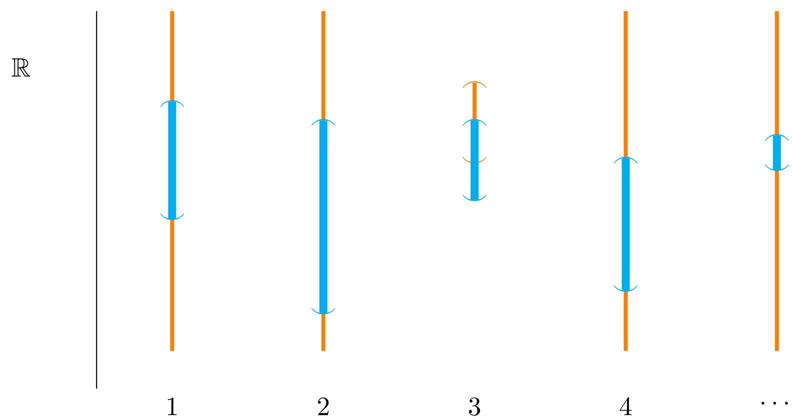
is called the *product topology* or the *Tychonoff topology.*

Sometimes it is more convenient work with the basis instead of the subbasis, that is

$$\beta = \left\{ \bigcap_{i\in J} \pi_i^{-1}(U_i) \mid J \subseteq I,\ J \text{ finite},\ U_i \in \tau_i \right\}.$$

If I is finite we have that $\tau_{Tych} = \tau_{Box}$ and if I is infinite $\tau_{Tych} \subseteq \tau_{Box}$. Next we show an example of the the strict inclusion in the last case:

Example 1.2.2. Consider $(X_i, \tau_i) = (\mathbb{R}, \tau_u)$ and $I = \mathbb{N}$.



In the box topology the basic open sets are functions whose values are inside the blue intervals. On the other hand, in the Tychonoff topology, the values of the functions can be in the whole real line, except for, at most, finitely many natural numbers, where values can be taken in bounded intervals, marked in orange. In this case it is clear that $\tau_{Tych} \subsetneq \tau_{Box}$.

Now we are going to prove that the topological space $(\prod_{i\in I} X_i, \tau_{Tych})$ is the product of $\{(X_i, \tau_i)\}_{i\in I}$ in the category of topological spaces. The two properties are satisfied.

Firstly, for all $i \in I$, the projection

$$\pi_i \colon \left(X = \prod_{i \in I} X_i, \tau_{Tych} \right) \to (X_i, \tau_i)$$

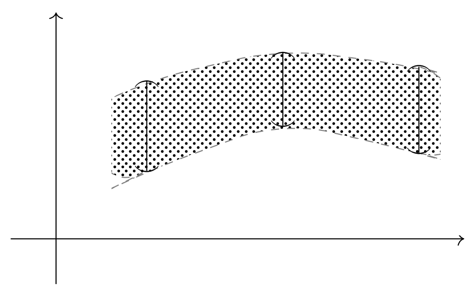
is continuous. In fact, given $U_i \in \tau_i$, $\pi_i^{-1}(U_i) \in \sigma \subseteq \beta_{Tych} \subseteq \tau_{Tych}$.

Secondly, given (Y, τ_i) and $(f_i \colon (Y, \tau_Y) \to (X_i, \tau_i))_{i \in I}$ a collection of continuous maps, the universal property is also satisfied, that is, there exists a unique continuous map $F \colon (Y, \tau_Y) \to (X, \tau_{Tych})$ that makes the following diagram commutative:

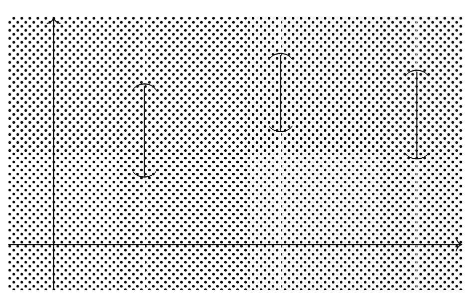
$$\begin{tikzcd}
(X, \tau_{Tych}) \arrow[r, "\pi_i"] & (X_i, \tau_i) \\
(Y, \tau_Y) \arrow[u, "F"] \arrow[ur, "f_i"'] &
\end{tikzcd}$$

The diagram being commutative means that the only way to define F is as follows: given $y \in Y$, then $F(y) \colon I \to \bigcup_{i \in I} X_i$, such that $F(y)(i) = f_i(y)$. Now we have to prove that F is continuous: given $\pi_i^{-1}(U_i) \in \sigma$, then $F^{-1}(\pi_i^{-1}(U_i)) \in \tau_i$ because f_i is continuous.

Remark. In the space $\mathbb{R}^{\mathbb{R}}$, the basic open sets in the box topology are formed by the functions with values in strips like the following one:



However, in the product topologies, the basic open sets are formed by functions which can take any real value except at finitely many points, where the values must be restricted in some open intervals, that is:



Hence, in τ_{Tych} the basic open sets are far bigger than in τ_{Box}.

Example 1.2.3. Consider $(\{0,1\}, \tau_{dis})$. Taking $(\{0,1\}^{\mathbb{N}}, \tau_{Box})$, notice that τ_{Box} is the discrete topology, and so it is a compact space if and only if it is finite. Using the binary expansion of the numbers in $[0,1]$, there is a bijection between $\{0,1\}^{\mathbb{N}}$ and the interval $[0,1]$, and hence it is infinite. In conclusion, $(\{0,1\}^{\mathbb{N}}, \tau_{Box})$ is not compact.

Chapter 2

Connectedness

2.1 Foundations

Definition 2.1.1. We say that a topological space (X, τ_X) is *disconnected* if there exist U, $V \in \tau_X$ such that $U \cup V = X$, $U \cap V = \varnothing$ and $U \neq \varnothing \neq V$.
We also say that $A \subseteq X$ is disconnected if there exist U, V open sets such that $A \subseteq U \cup V$, $A \cap U \cap V = \varnothing$ and $A \cap U \neq \varnothing \neq A \cap V$.

Examples 2.1.2. (1) (X, τ_{ind}) is a connected topological space, since the unique open sets are the empty-set and X.

(2) $(\mathbb{R}, \tau_{Kol})$ is a connected topological space.

(3) Take (X, τ_{dis}) the discrete topological space. Then $A \subseteq X$ is connected if and only if $|A| \leq 1$.

(4) Let $(\mathbb{Q}, \tau_u)$ be the topological space. $A \subseteq \mathbb{Q}$ is connected if and only if $|A| \leq 1$.

(5) Let $(\mathbb{R}, \tau_{Sor})$ be the Sorgrenfrey line. $A \subseteq \mathbb{R}$ is connected if and only if $|A| \leq 1$.

Proof. We will only prove part (4) because the other ones are very similar.
$\Leftarrow$) The empty-set and the one-point sets are connected.
$\Rightarrow$) By contradiction, suppose that $|A| \geq 2$. Then there exist $x \leq y \in A$, and using that the set of irrational numbers is dense, there exists $z \in \mathbb{I}$ such that $x < z < y$. Take $U = (-\infty, z) \cap \mathbb{Q}$, $V = (z, \infty) \cap \mathbb{Q} \in \tau_u$. Clearly, $A \subseteq U \cup V$, $A \cap U \cap V = \varnothing$ and $A \cap U \neq \varnothing \neq A \cap V$. Therefore, A is disconnected. $\square$

The following properties about connectedness are well-known:

Proposition 2.1.3 (Properties of connectedness)**.** *Let (X, τ) be a topological space and $A \subseteq X$.*

(i) *If A is connected and $A \subseteq B \subseteq \overline{A}$, then B is also connected.*

(ii) *Let* $\{A_i\}_{i\in I}$ *be a collection of connected sets such that* $\bigcap_{i\in I} A_i \neq \varnothing$. *Then* $\bigcup_{i\in I} A_i$ *is connected. Moreover, if there exists* A_{i_0} *such that* $A_{i_0} \cap A_i \neq \varnothing$ *for all* $i \in I$, $\bigcup_{i\in I} A_i$ *is also connected.*

(iii) *If* f *is a continuous map between the topological spaces* (X, τ_X) *and* (Y, τ_Y) *and* A *is a connected set in the first one, then* $f(A)$ *is connected in the second topological space. Hence connectedness is a topological property.*

(iv) *Let* $\{(X_i, \tau_i)\}_{i=1}^n$ *be a set of topological spaces. Then* $(\prod_{i=1}^n X_i, \tau_{Box})$ *is connected if and only if* (X_i, τ_i) *is connected, for all* $i \in \{1, \dots, n\}$.

In the infinite case, the property (iv) does not hold, as we will now see:

Example 2.1.4. If $(\prod_{i\in I} X_i, \tau_{Box})$ is connected, since the projections are continuous, we obtain that (X_i, τ_i) is connected, for all $i \in I$. However, the converse implication is not true. Let us give a counterexample.
Let us take $(X_i, \tau_i) = (\mathbb{R}, \tau_u)$ for each $i \in I = \mathbb{R}$ and $(\mathbb{R}^{\mathbb{R}}, \tau_{Box})$. Define

$$U = \{\phi \in \mathbb{R}^{\mathbb{R}} \mid \phi \text{ is bounded}\} \quad \text{and} \quad U = \{\phi \in \mathbb{R}^{\mathbb{R}} \mid \phi \text{ is unbounded}\}$$

We will show that both U and V are open sets. Let $\phi \in U$. Then ϕ is bounded. Defining for each $\varepsilon > 0$

$$U_\varepsilon = \{\psi \in \mathbb{R}^{\mathbb{R}} \mid \psi(x) \in (\phi(x) - \varepsilon, \phi(x) + \varepsilon)\},$$

we obtain that $\psi \in U_\varepsilon \subseteq U$, so U is open. In the same way it can be proved that V is open.
Now, we conclude that there exist U, V open sets such that $U \cup V = \mathbb{R}^{\mathbb{R}}$, $U \cap V = \varnothing$ and $U \neq \varnothing \neq V$; that is, $(\mathbb{R}^{\mathbb{R}}, \tau_{Box})$ is not connected.

However, with the Tychonov topology we certainly achieve that if $\{(X_i, \tau_i)\}_{i\in I}$ is a family of connected spaces, then so is $(\prod_{i\in I} X_i, \tau_{Tych})$:

Theorem 2.1.5. *Let* $\{(X_i, \tau_i)\}_{i\in I}$ *be a family of connected topological spaces, then* $(\prod_{i\in I} X_i, \tau_{Tych})$ *is a connected topological space.*

Proof. For notation simplicity let $\prod_{i\in I} X_i = X$. Fix an element $\varphi_0 \in X$, that is,

$$\varphi_0 \colon I \to \bigcup_{i\in I} X_i \text{ such that } \varphi_0(i) \in X_i, \text{ for all } i \in I,$$

and define

$$D = \bigcup\{C \subseteq X \mid C \text{ connected such that } \varphi_0 \in C\}.$$

Since D is the union of connected elements with non-empty intersection (note that all of them intersect at φ_0) D is connected.

D is also dense. Indeed, for a finite $J \subseteq I$ take

$$B = \bigcap_{i\in J} \pi_i^{-1}(U_i) \in \beta_{Tych} \quad \text{and} \quad x_i \in U_i \text{ for each } i \in J.$$

Consider the set

$$A = \{\varphi \in X \mid \varphi_0(i) = \varphi(i)\ \forall i \notin J \text{ and } \varphi(i) \in X_i\ \forall i \in J\}.$$

A is homeomorphic to $\prod_{i \in J} X_i$ which is a *finite* product of topological spaces, and this is connected. Hence, A is connected and $\varphi_0 \in A$, so $A \subseteq D$. Moreover, $\varphi^* \in A \cap B$, where

$$\varphi^* \colon I \to \bigcup_{i \in I} X_i \text{ such that } \varphi^*(i) = \begin{cases} \varphi_0(i), & \text{if } i \notin J, \\ x_i, & \text{if } i \in J. \end{cases}$$

Hence, $\varnothing \neq A \cap B \subseteq D \cap B$ for all $B \in \beta_{Tych}$, so D is dense. Finally, since D is connected, the closure $\overline{D} = X$ is connected. □

2.2 Order topologies

We start recalling some properties about ordered sets and use them to define the order topology.

Definition 2.2.1. Let X be a set and $\leq$ a relation on X. It is said that $\leq$ is an *order relation* and $(X, \leq)$ a *partially ordered set* or *ordered set*, if it has these properties:

(i) $\leq$ is *reflexive*: $x \leq x$, $\forall x \in X$.

(ii) $\leq$ is *antisymmetric*: $x \leq y$ and $y \leq x \implies x = y$, $\forall x, y \in X$

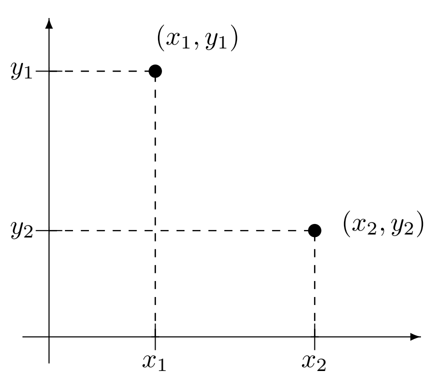
(iii) $\leq$ is *transitive*: $x \leq y$ and $y \leq z \implies x \leq z$, $\forall x, y, z \in X$.

Furthermore, if for all $x, y \in X$ we have $x \leq y$ or $y \leq x$, we say that $(X, \leq)$ is a *total order relation*.

Example 2.2.2 ($\mathbb{R}^2$ with the lexicographic order)**.** We define the lexicographic order in the next way: take $\boldsymbol{x} = (x_1, x_2)$ and $\boldsymbol{y} = (y_1, y_2) \in \mathbb{R}^2$, then:

$$\boldsymbol{x} \leq \boldsymbol{y} \iff x_1 < y_1 \text{ or } (x_1 = y_1 \text{ and } x_2 \leq y_2)$$

Here, $\boldsymbol{x} \leq \boldsymbol{y}$:



Definition 2.2.3. Let $(X, \leq)$ be a partially ordered set and $A \subseteq X$. Then $x \in X$ is an upper bound of A if $a \leq x$ for all $a \in A$.

Using that definition it can be considered the set

$$A^u = \{x \in X \mid x \text{ is a upper bound of } A\}$$

and its dual

$$A^l = \{x \in X \mid x \text{ is a lower bound of } A\}.$$

These sets are useful in order to define the supremum.

Definition 2.2.4. Let $(X, \leq)$ be an ordered set and $A \subseteq X$. Then $x \in X$ is a *supremum* of A if $x \in A^u$ and for all $y \in A^u$ $x \leq y$.

There are also two properties that an orden relation $(X, \leq)$ can hold: to be Dedekind complete and to be dense respect to the order.

Definition 2.2.5. Let $(X, \leq)$ be an ordered set, then $(X, \leq)$ is *Dedekind complete* if any non-empty and bounded subset of X has a supremum.

Definition 2.2.6. Let $(X, \leq)$ be an ordered set, then $(X, \leq)$ is *dense respect to the order* or *order-dense* if

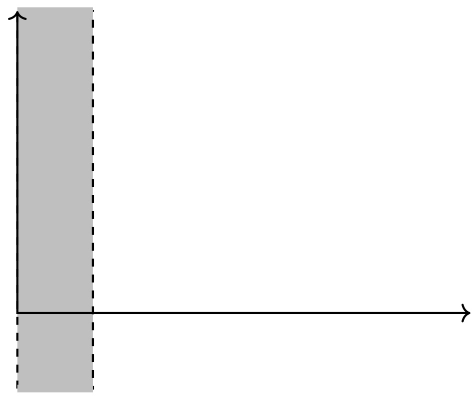
$$x < y \in X \implies \exists z \in X \text{ such that } x < z < y$$

Definition 2.2.7. Let $(X, \leq)$ be a ordered set, then $(X, \leq)$ is a *linear continuum* if $(X, \leq)$ is Dedekind complete and dense respect to the order.

Let us see some examples of Dedekind complete and order-dense sets. With these examples one can see that the previous properties are independent to each other.

Examples 2.2.8. (1) $(\mathbb{R}, \leq)$ is Dedekind complete and dense with respect to the usual order.

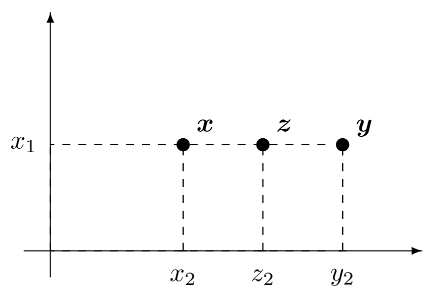
(2) $(\mathbb{R}^2, \leq_{lex})$ is not Dedekind complete. For example, $A = (0,1) \times \mathbb{R}$ is bounded, because, for any $\boldsymbol{x} \in A$, we have: $\boldsymbol{x} \leq_{lex} (1, a)$, for any $a \in \mathbb{R}$. But A has not a supremum in $\mathbb{R}^2$. Indeed, suppose by contradiction that (x, y) is the supremum of A. Thus, $x \leq 1$ and we shall distinguish two cases. If $x < 1$, there exists $x' \in (0,1)$ greater than x and $(x', y) \in A$ would be greater than (x, y), which is a contradiction. On the other hand, if $x = 1$, then $(1, y-1) < (x, y)$ is a smaller point and is also an upper bound, so (x, y) can not be the supremum.

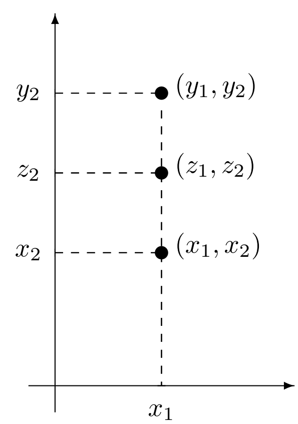


However, $(\mathbb{R}^2, \leq_{lex})$ is dense with respect to the order. Take, $\boldsymbol{x} = (x_1, x_2), \boldsymbol{y} = (y_1, y_2) \in \mathbb{R}^2$ and suppose without loss of generality that $x_1 \leq x_2$. Then there are two possibilities:

1. If $x_1 < y_1$ choose $\boldsymbol{z} = (z_1, z_2) \in X$ such that $z_1 = \frac{x_1+y_1}{2}$, then $\boldsymbol{x} \leq_{lex} \boldsymbol{z} \leq_{lex} \boldsymbol{y}$.

2. If $x_1 = y_1$ choose $\boldsymbol{z} = (z_1, z_2) \in X$ such that $z_1 = x_1$ and $z_2 = \frac{x_2+y_2}{2}$, then $\boldsymbol{x} \leq_{lex} \boldsymbol{z} \leq_{lex} \boldsymbol{y}$.



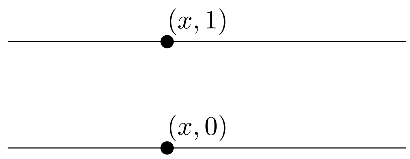


(3) $([0,1]^2, \leq_{lex})$ is a linear continuum.
It is dense with respect to the other by the previous argument, because $[0,1]^2 \subseteq \mathbb{R}^2$. In order to see that it is Dedekind complete take $A \subseteq [0,1]^2$ bounded by $\boldsymbol{a}$. Define, $A_1 = \{x_1 \mid \boldsymbol{x} = (x_1, x_2) \in A\}$ and call a_1 its supremum (remember that $(\mathbb{R}, \leq)$ is Dedekind complete and $A_1 \subseteq \mathbb{R}$). Then there are two possibilities:

1. If $(\{a_1\} \times [0,1]) \cap A = \varnothing$, $(a_1, 0)$ is the supremum of A.

2. If $(\{a_1\} \times [0,1]) \cap A \neq \varnothing$. Define, $B_2 = \{x_2 \mid \boldsymbol{x} = (x_1, x_2) \in \{a_1\} \times [0,1]\}$ and call b_2 its supremum. Then (a_1, b_2) is the supremum of A.

(4) $(\mathbb{R} \times \{0,1\}, \leq_{lex})$ is Dedekind complete, by the same argument, but is not dense respect to the order. For example, for each $x \in \mathbb{R}$ there is no $\boldsymbol{z} = (z_1, z_2) \in \mathbb{R} \times \{0,1\}$, such that $(x,0) <_{lex} (z_1, z_2) <_{lex} (x,1)$ for all



Now we will see that connectedness is intrinsically related to the order properties. Firstly, starting from a totally ordered set $(X, \leq)$, we will construct a topology, namely the order topology. Then we will show under which conditions is the corresponding space connected. In particular, as we shall see, the results that follow can be applied to $\mathbb{R}$ with the usual order, because the order topology obtained from it is, in fact, the usual topology. Furthermore, it will always be useful to have $\mathbb{R}$ with the usual order in mind, because the idea of some of the arguments that we will use is very similar to the ones that are normally used when dealing concretely with $(\mathbb{R}, \tau_u)$, which is for sure very familiar to the reader. Let's start introducing some notation and the order topology:

Notation. Let $(X, \leq)$ be a totally ordered set. For all $x \in X$ define the following sets:

$$(\leftarrow, x) = \{z \in X \mid z < x\}$$
$$(x, \rightarrow) = \{z \in X \mid z > x\}$$

We shall also use $(x,y), (x,y], [x,y)$ and $[x,y]$ with the usual meaning.

Definition 2.2.9. Define the set $\sigma = \{(\leftarrow, x) \mid x \in X\} \cup \{(x, \rightarrow) \mid x \in X\}$, which is a subset of $\mathcal{P}(X)$. The *order topology induced by* $(X, \leq)$ is the topology generated by σ (i.e. the topology which has σ as subbase), which we shall denote $\tau_{\leq} = \langle \sigma \rangle$. A straight consequence is that the base of this topology is given by $\beta_{\leq} = \{(a,b) \subset X \mid a, b \in X, a < b\} \cup \sigma$, because

$$\Big(\bigcap_{i=1}^{n} (a_i, \rightarrow)\Big) \bigcap \Big(\bigcap_{j=1}^{m} (\leftarrow, b_j)\Big) = \Big(\max_{1 \leq i \leq n} a_i, \min_{1 \leq j \leq m} b_j\Big).$$

Examples 2.2.10. In order to get used, let's study a little bit the topologies generated by some of the most common totally ordered sets:

(1) The order topology generated by $(\mathbb{R}, \leq_u)$ (the real numbers with the usual order) is the usual topology. Indeed, in this case the basic open sets we obtain are of the form (a,b) with $a < b$ in the usual order, so $\beta_{\leq}$ is clearly a base of the usual topology.

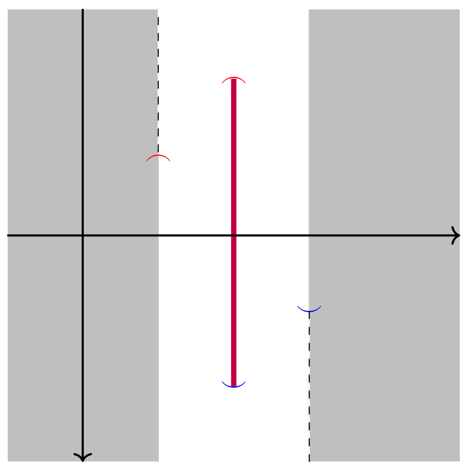
(2) If we consider $(\mathbb{R}^2, \leq_{lex})$, it turns out that $\tau_{\leq_{lex}} = \tau_{dis} \times \tau_u$ (where both

topologies are thougth for $\mathbb{R}$). To see this, it is enough to point that in the finite product of topologies the basic open sets are obtained as cartesian products of one basic open set of each of the topologies, so in this case we can consider products of singletons (basic opens in τ_{dis}) and open intervals (basic opens in τ_u). Thus, it is clear that if $b_1 < b_2$, then

$$((a,b_1),(a,b_2)) = \{a\} \times (b_1,b_2),$$

so the basic opens of the product are contained in $\beta_{\leq}$. Moreover, it is clear that those sets form in fact a basis of $\tau_{\leq}$, because given $(x,y) \in ((a_1,b_1),(a_2,b_2)) \in \beta_{\leq}$, taking a suitable $\varepsilon > 0$ we have:

$$(x,y) \in \{x\} \times (y-\varepsilon, y+\varepsilon) \subset ((a_1,b_1),(a_2,b_2)).$$



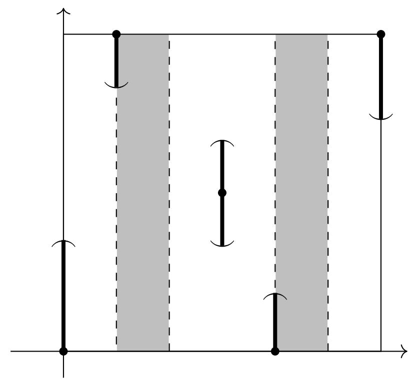
Following the previous example, in the case of $([0,1]^2, \leq_{lex})$ we can restrict to four types of basic open sets in the order topology (with $a, b_1, b_2 \in [0,1]$):

1. Sets of the form $\{a\} \times (b_1,b_2)$, which are "the best" neighborhoods of points (a,b) with $b \in (b_1,b_2)$.

2. Sets of the form $\{0\} \times [0,a)$, which are clearly neighborhoods of $(0,0)$.

3. Sets of the form $\{1\} \times (a,1]$, which are neighborhoods of $(1,1)$.

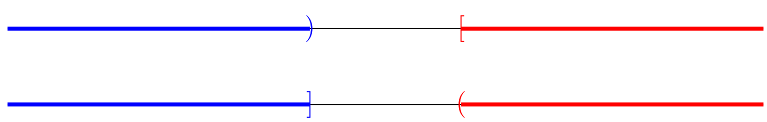
4. Sets of the form $(a,a+\varepsilon) \times [0,1] \cup \{a\} \times (b_1,1] \cup \{a+\varepsilon\} \times [0,b_2)$. The neighborhoods of the points located in the "roof" (second coordinate equal 1) or the "floor" (second coordinate equal 0) are of this form.



(3) Finally, if we consider $(\mathbb{R} \times \{0,1\}, \leq_{lex})$, the subbasic open sets are of the form

1. $((a,0),\rightarrow) = (a,+\infty) \times \{0\} \cup [a,+\infty) \times \{1\}$;
2. $((a,1),\rightarrow) = (a,+\infty) \times \{0\} \cup (a,+\infty) \times \{1\}$;
3. $(\leftarrow,(b,0)) = (-\infty,b) \times \{0\} \cup (-\infty,b) \times \{1\}$;
4. $(\leftarrow,(b,1)) = (-\infty,b] \times \{0\} \cup (-\infty,b) \times \{1\}$;

with $a, b \in \mathbb{R}$.



Now, we will state and prove a theorem that charaterizes completely the connectedness of a topology induced by an order in terms of the properties of the order.

Theorem 2.2.11. *Let $(X, \leq)$ be a totally ordered set and $\tau_{\leq}$ the order topology induced. Then $(X, \tau_{\leq})$ is connected if and only if $(X, \leq)$ is a linear continuum.*

Proof. $\Rightarrow$) We shall proof this implication by contraposition.

Suppose that $(X, \leq)$ is not order-dense. Take x and y in X (we can suppose that $x < y$) such that there does not exist $z \in X$ satisfying $x < z < y$. Then the sets $(\leftarrow, y)$ and $(x, \rightarrow)$ are clearly open in $(X, \tau_{\leq})$ and their union is the whole space (because $x < y$). Moreover, $(\leftarrow, y) \cap (x, \rightarrow) = (x, y) = \varnothing$ by the choice of x and y, so $(X, \tau_{\leq})$ is disconnected.

Suppose that $(X, \leq)$ is not Dedekind-complete. Take $A \subset X$ nonempty, upper bounded and with no supremum. We can define the open sets

$$U := \bigcup_{a \in A} (\leftarrow, a) \quad \text{and} \quad V := \bigcup_{b \in A^u} (b, \rightarrow),$$

because A and A^u are nonempty. We shall see that they disconnect the space.

First, it clearly follows from the definition that A^u is not included in U and A is not included in V, so none of them are the total set. Let $x \in X \setminus V$. Since A has no supremum, if x were an upper bound of A there would be another upper bound $b < x$ and thus $x \in (b, \rightarrow) \subset V$, which is not possible by assumption. Therefore, x does not belong to A^u and there exists $a \in A$ greater than x, so $x \in (\leftarrow, a) \subset U$. This proves that $U \cup V = X$ and both are proper subsets.

Finally, let's show that $U \cap V = \varnothing$. If v belongs to V, then $v \in (b, \rightarrow)$ for some $b \in A^u$ and therefore v is also an upper bound. But we have said that A^u is not included in U, so v cannot be inside U.

$\Leftarrow$) By contradiction, suppose that there exist U, V nonempty, disjoint and open such that their union is the whole space. Without loss of generality we can take $x \in U$ and $y \in V$ satisfying $x < y$. Then define the sets $A = [x, y]$ and $B = \{z \in X \mid [x, z) \subset U\}$. Since U is open, $B \neq \varnothing$ and it is upper bounded by y. Therefore, by Dedekind-completeness there exists $c \in [x, y]$ supremum of B, which must be inside U or V.

If $c \in U$, there would be an open neighborhood of c inside U and due to the order density there would be points greater (with our order) than c but smaller (with our order) than y in such neighboorhood, so c wouldn't be the supreme of B, contradiction.

If $c \in V$, there would be an open neighborhood of c inside V and due to the order density there would be points smaller (with our order) than c but greater (with our order) than x in such neighboorhood. Since those points would be in V, they wouldn't be in U, but that's a contradiction with the fact that $[x, c) \subset U$. □

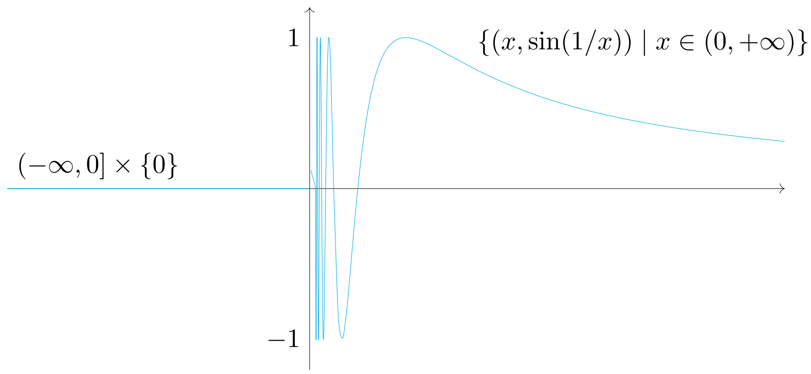
Taking into account that the unique linear continuum subsets of $\mathbb{R}$ with the usual order are intervals and the properties of Tychonov topology, it is crystal clear the following corollary:

Corollary 2.2.12. *A subspace S of $(\mathbb{R}, \tau_u)$ is connected if and only if S is an interval. Thus, if I is a set of indexes (finite or infinite), $(\mathbb{R}^I, \tau_{Tych})$ is also connected.*

A trivial consequence of the corollary is that the graph of a continuous map defined in an interval must be connected. We can use that to show that the topologist's sine

$$A = \{(x, \sin(1/x) \in \mathbb{R}^2 \mid x \in (0, +\infty)\} \,\dot{\cup}\, (-\infty, 0] \times \{0\} = A_1 \,\dot{\cup}\, A_2$$

is connected. Indeed, it's clear that both parts are connected, but their union is disjoint, so it is not straightforward. However, point that $A_2 \subset A_2 \cup \{(0,0)\} \subset \overline{A_2}$, so $A_2 \cup \{(0,0)\}$ is connected, by Proposition 2.1.3. Moreover, $A_1 \,\dot{\cup}\, A_2 = A_1 \cup (A_2 \cup \{(0,0)\})$ and in the second case the union is not disjoint, so the union is connected.



Finally, according to what we have seen before, it also follows that $([0,1]^2, \tau_{\leq_{lex}})$ is connected, but $(\mathbb{R}^2, \tau_{\leq_{lex}})$ and $(\mathbb{R} \times \{0,1\}, \tau_{\leq_{lex}})$ are not.

2.3 Connected components

Definition 2.3.1. Let (X, τ) be a topological space. For each $x \in X$, we define

$$C(x) = \bigcup\{C \subseteq X \mid x \in C, C \text{ is connected}\}.$$

The set $C(x)$ is called the *connected component* of x.

The following proposition justifies the use of the name connected:

Proposition 2.3.2 (Properties of connected components)**.** *Let (X, τ) be a topological space and $x \in X$. Then*:

(i) *The connected component $C(x)$ is the biggest connected set containing x;*

(ii) *Connected components are closed;*

(iii) *the connected components form a partition of X;*

(iv) *(X, τ) is connected if and only if there is exactly one connected component.*

Proof. (i) $C(x)$ is the union of connected sets whose intersection is non-empty, so by Proposition 2.1.3 it follows that $C(x)$ is connected. Let C be a connected set including x. It is clear that $C \subseteq C(x)$ and so the connected component is the biggest connected set containing x.

(ii) We have that $x \in \overline{C(x)}$ and by Proposition 2.1.3, $\overline{C(x)}$ is connected. Since $C(x)$ is the biggest connected set containing x, we have that $\overline{C(x)} \subseteq C(x)$ and hence $C(x)$ is closed.

(iii) We have to see that whenever two connected components have non-empty intersection, they are equal. Assume that $C(x) \cap C(y) \neq \varnothing$. Then by Proposition 2.1.3, $C(x) \cup C(y)$ is connected. Since $x \in C(x) \cup C(y)$ and $C(x)$ is the biggest connected set containing x, we get $C(y) \subseteq C(x) \cup C(y) \subseteq C(x)$ and similarly

$C(x) \subseteq C(y)$, so $C(x) = C(y)$.

(iv) If X is connected, it is clear that $C(x) = X$ for all $x \in X$. Assume now that we only have one connected component. Since connected components form a partition, $C(x) = X$ for all $x \in X$ and so X is connected. $\square$

Since the connected components form a partition, we always have a equivalence relation,

$$x \sim y \iff C(x) = C(y),$$

which we shall use later.

Example 2.3.3. In the topological space $\left(\{\frac{1}{n} \mid n \in \mathbb{N}\} \cup \{0\}, \tau_u\right)$ we have that $C\left(\frac{1}{n}\right) = \{\frac{1}{n}\}$ and since the connected components form a partition, $C(0) = \{0\}$.

2.4 Total disconnection

Definition 2.4.1. A topological space (X, τ) is said to be *totally disconnected* if $C(x) = \{x\}$ for all $x \in X$.

We have seen in Example 2.1.2 that the unique connected sets in a discrete topological space are the singletons and the empty set. Hence, $C(x) = \{x\}$ for all $x \in X$ and (X, τ_{dis}) is totally disconnected. Nevertheless, the converse is not true, as the following examples show:

Examples 2.4.2.

(1) By Example 2.1.2, $(\mathbb{Q}, \tau_u)$ is totally disconnected.

(2) Using Example 2.1.2 again, $(\mathbb{R}, \tau_{Sor})$ is totally disconnected.

The next proposition shows a natural way of constructing totally disconnected spaces starting from an arbitrary topological space.

Proposition 2.4.3. *Let (X, τ) be a topological space and consider the equivalence relation given by*

$$x \sim y \iff C(x) = C(y)$$

Then the space $(X/\!\sim, \tau_{quot})$ is totally disconnected.

Proof. By way of contradiction assume that there exists a connected set $C \subseteq X/\!\sim$ such that $|C| \geq 2$. Then $p^{-1}(C)$ is disconnected: otherwise,we would have $p^{-1}(C) \subseteq C(x)$ for some $x \in X$ and so $C = pp^{-1}(C) \subseteq \{p(x)\}$, contradicting that $|C| \geq 2$. Then there exist $F, G \subseteq X$ two closed sets disconnecting $p^{-1}(C)$, that is,

$$\begin{cases} p^{-1}(C) \subseteq F \cup G \\ p^{-1}(C) \cap F \cap G = \varnothing \\ p^{-1}(C) \cap F \neq \varnothing \neq p^{-1}(C) \cap F. \end{cases}$$

Let $x \in p^{-1}(C)$. Since $C(x)$ is connected, $C(x) \subseteq F \cup G$ and $C(x) \cap F \cap G = \varnothing$, we have $C(x) \cap F = \varnothing$ or $C(x) \cap G = \varnothing$, that is, $C(x) \subseteq F$ or $C(x) \subseteq G$. Since $x \in p^{-1}(C)$, we have $C(x) \subseteq p^{-1}(C)$, so it follows that $C(x) \subseteq F \cap p^{-1}(C)$ or $C(x) \subseteq G \cap p^{-1}(C)$. Hence,

$$F \cap p^{-1}(C) = \bigcup_{x \in F \cap p^{-1}(C)} C(x) \quad \text{and} \quad G \cap p^{-1}(C) \bigcup_{x \in G \cap p^{-1}(C)} C(x)$$

Now, $F \cap p^{-1}(C)$ and $G \cap p^{-1}(C)$ are non-empty, so $p(F \cap p^{-1}(C))$ and $p(G \cap p^{-1}(C))$ are also non-empty, closed and disjoint. Thus they form a disconnection of C which is a contradiction because C was connected. Hence the quotient space is totally disconnected. $\square$

Considering the same equivalence relation, the totally disconnected spaces satisfy the following universal property:

Proposition 2.4.4. *Given a totally disconnected topological space (Y, τ_Y) and a continuous map $f\colon (X, \tau_X) \to (Y, \tau_Y)$ there exists a unique continuous map $\hat{f}\colon (X/{\sim}, \tau_{quot}) \to (Y, \tau_Y)$ such that the following diagram commutes:*

$$\begin{tikzcd}
(X, \tau_X) \arrow[r, "f"] \arrow[d, "p"'] & (Y, \tau_Y) \\
(X/{\sim}, \tau_{quot}) \arrow[ur, dashed, "\hat{f}"'] &
\end{tikzcd}$$

Proof. Define $\hat{f}(p(x)) = f(x)$. We have to see that it is well-defined: assume that $p(x) = p(y)$. Our aim is to show that $f(x) = f(y)$. Since $p(x) = p(y)$ we have that $C(x) = C(y)$. Then $f(x), f(y) \in f(C(x))$ and $f(C(x))$ is a connected set so $|f(C(x))| = 1$. It follows that $f(x) = f(y)$.

Now we see that $\hat{f}$ is continuous. Let $F \in \mathcal{C}_Y$. We will prove that $\hat{f}^1(F) \in \mathcal{C}_{quot}$. We have that

$$\hat{f}^{-1}(F) = \{p(x) \in X/{\sim} \mid f(x) \in F\} = p(f^{-1}(F))$$

and $p(f^{-1}(F)) \in \mathcal{C}_{quot}$ if and only if $p^{-1}pf^{-1}(F) \in \mathcal{C}_X$. Since f is continuous, $p^{-1}pf^{-1}(F) = f^{-1}(F) \in \mathcal{C}_X$, and $\hat{f}$ is continuous. $\square$

2.5 Path-connectedness

Definition 2.5.1. Given a topological space (X, τ_X) and given two points $x, y \in X$, a *path* is a continuous map $\sigma_{xy}\colon [0,1] \to X$ such that $\sigma_{xy}(0) = x$ and $\sigma_{xy}(1) = y$.

We can consider the trivial path $\sigma_{xx}(t) = x$ for each $t \in [0,1]$, and we can also consider the inverse path, that is, given a path σ_{xy} that connects x and y, the inverse path is defined by $\sigma_{xy}^{-1}\colon [0,1] \to X$ such that $\sigma_{xy}^{-1}(t) = \sigma_{xy}(1-t)$.

We can also do the composition of two paths: Given two paths σ_{xy} and σ_{yz} the composition is the path $\sigma_{xz}\colon [0,1] \to X$ where

$$\sigma_{xz}(t) = \begin{cases} \sigma_{xy}(2t) & \text{if } t \in [0, \frac{1}{2}] \\ \sigma_{yz}(2t-1) & \text{if } t \in [\frac{1}{2}, 1]. \end{cases}$$

σ_{xz} is a continuous map.

Then taking this previous facts into consideration we have the following equivalence relation:

$$x \sim y \iff \text{there exist a path that connects } x \text{ and } y.$$

Definition 2.5.2. A topological space (X, τ_X) is *path-connected* if for all $x, y \in X$ there exist a path that connects them. Given $A \subseteq X$, A is path-connected if (A, τ_A) is path-connected.

The following proposition gives the relation between connectedness and path-conectedness.

Proposition 2.5.3. *Let (X, τ_X) a topological space. If (X, τ_X) is path-connected, then (X, τ_X) is connected.*

Proof. Take $x_0 \in X$. Then for all $x \in X$ there exists a path σ_{x_0x} such that $\sigma_{x_0x}([0,1])$ is connected (because it is the image of a connected set by a continuous map, see Proposition 2.1.3). Since $x_0 \in \bigcap_{x\in X} \sigma_{x_0x}([0,1])$, then $\bigcup_{x\in X} \sigma_{x_0x}([0,1])$ is connected by Proposition 2.1.3, and $\bigcup_{x\in X} \sigma_{x_0x}([0,1]) = X$, so X is connected. $\square$

Now we can consider the next examples to show that the other implication is not necessarily true.

Examples 2.5.4. (1) Take $([0,1]^2, \tau_{\leq_{lex}})$. It is connected but we are going to see that it is not path-connected. Suppose by contradiction that it is path-connected. Then there exist a path, say σ, that connects $(0,0)$ and $(1,1)$.

Now recall that if we have a continuous map $f\colon X \to Y$, then for all $A \subseteq X$, $f(\overline{A}) \subseteq \overline{f(A)}$. Furthermore, if $D \subseteq X$ is dense then $f(X) = f(\overline{D}) \subseteq \overline{f(D)}$ and if f is also a surjective map then $f(D)$ is dense.

In our case σ is a continuous map and it is also surjective. For if not, there exists $(x,y) \in [0,1]^2$ such that $(x,y) \notin \sigma([0,1])$. This implies that

$$\begin{cases} \sigma([0,1]) \subseteq (\leftarrow, (x,y)) \cup ((x,y), \rightarrow) \\ \sigma([0,1]) \cap (\leftarrow, (x,y)) \cap ((x,y), \rightarrow) = \varnothing \\ (0,0) \in \sigma([0,1]) \cap (\leftarrow, (x,y)) \neq \varnothing \\ (1,1) \in \sigma([0,1]) \cap ((x,y), \rightarrow) \neq \varnothing \end{cases}$$

so $\sigma([0,1])$ is not connected, which is a contradiction. Then σ is surjective.

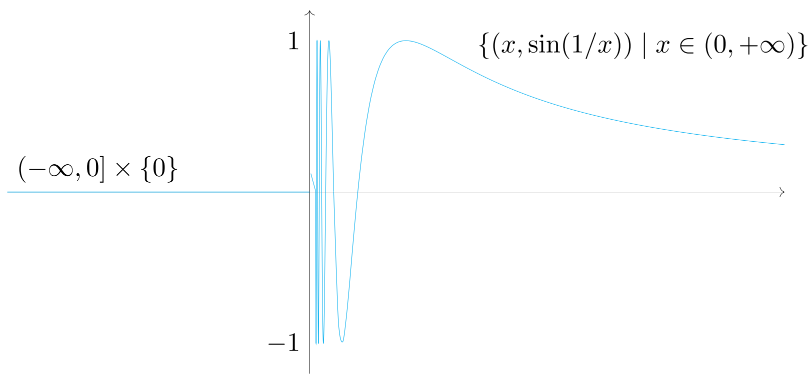
Now consider the set $D = [0,1] \cap \mathbb{Q}$. By the previous comments, $\sigma(D)$ is dense and it is also countable (since $\#\sigma(D) \leq \#D$). For all $x \in [0,1]$, $\{x\} \times (0,1)$ is an open set, and since $\sigma(D)$ is dense, then $\sigma(D) \cap (\{x\} \times [0,1]) \neq \varnothing$, so there exists $(x, \sigma(t_x)) \in \sigma(D) \cap (\{x\} \times [0,1])$. Then we have

$$\{(x, \sigma(t_x)) \mid x \in [0,1]\} \subseteq \sigma(D)$$

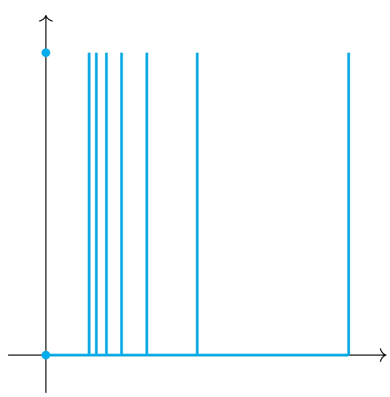
and since the first set is not countable and the second set is, then we have a contradiction. So $([0,1]^2, \tau_{\leq_{lex}})$ is not path-connected.

(2) Consider the topological space $(\mathbb{R}^2, \tau_u)$ and the following sets:

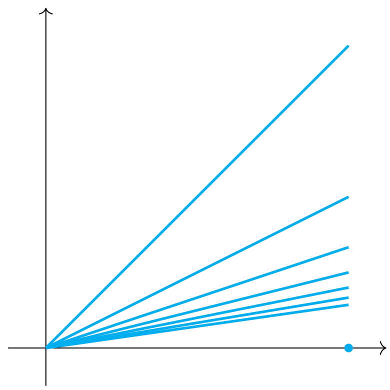
(a) $A = \{(x, \sin\frac{1}{x}) \mid x \in (0,\infty)\} \cup ((-\infty, 0] \times \{0\})$, the *topologist's sine*.



(b) The *comb space*: $(\{0\} \times \{0,1\}) \cup (K \times [0,1]) \cup ([0,1] \times \{0\})$ where $K = \{\frac{1}{n} \mid n \in \mathbb{N}\}$



(c) The *broom space*: It is the subset of $\mathbb{R}^2$ that consists of all closed line segments joining the origin to the point $(1, \frac{1}{n})$ where $n \in \mathbb{N}$ together with the point $(1,0)$.



All of them are connected, but none is path-connected.

Now we are going to see some properties of the path-connected sets. Most of them are also true for connected sets.

Proposition 2.5.5. *Let (X, τ_X) and (Y, τ_Y) be two topological spaces.*

(i) *The image of a path-connected set by a continuous map is also a path-connected set.*

(ii) *Path-connectedness is a divisible property.*

(iii) *Path-connectedness is a topological property.*

(iv) *If $f\colon (X, \tau_X) \to (Y, \tau_Y)$ is a continuous map and (X, τ_X) is path-connected, then $(G_f \subseteq X \times Y, \tau_{tyc})$ is path-connected, where $G_f = \{(x, f(x)) \mid x \in X\}$.*

(v) *The union of path-connected sets with non-empty intersection is path-connected.*

(vi) *Let consider the topological space $(\mathbb{R}, \tau_u)$ and let $A \subseteq \mathbb{R}$, then A is path-connected if and only if A is connected.*

Proof. We will only prove part (vi) because the other ones are easy.
The right implication is always true, and for the other implication notice that $A \subseteq \mathbb{R}$ is connected if and only if A is an interval ($[x, y] \subseteq A$ whenever $x, y \in A$), and these ones are always path-connected, given two points x and y in the interval consider the path σ_{xy} such that $\sigma_{xy}(t) = x + t(y - x)$ for each $t \in [0, 1]$. $\square$

The next example shows that a property (see Proposition 2.1.3) of connectedness fails in path-connectedness.

Example 2.5.6. The closure of a path-connected set is not necessarily path-connected. For example, if we consider $\{(x, \sin \frac{1}{x}) \mid x \in (0, \infty)\}$, it is connected and it is also path-connected (applying Proposition 2.5.5 (iv) it can be seen as a graph of a continuous map defined in a connected set), but its closure is not path-connected.

2.5.1 Path-connected components

Definition 2.5.7. Let (X, τ_X) be a topological space and recall that we have the equivalence relation

$$x \sim y \quad \Longleftrightarrow \exists\, \sigma_{xy} : [0,1] \to X \text{ such that } \sigma_{xy}(0) = x,\ \sigma_{xy}(1) = y$$

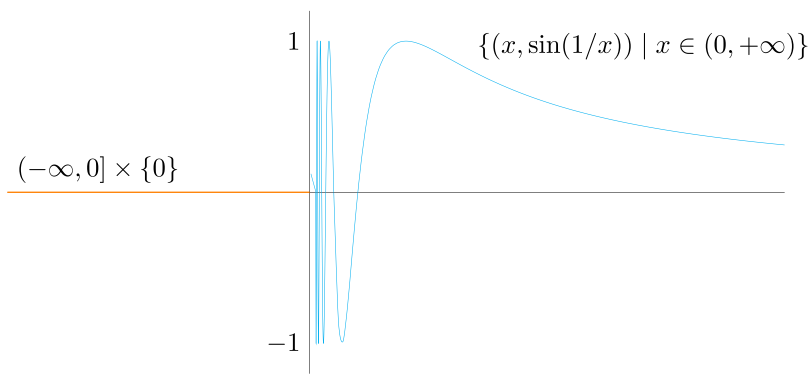
Then for all $x \in X$ the class of equivalence $c(x)$ is called the *path-connected component* of x.

Path-connected components form a partition of X: $\{c(x) \mid x \in X\}$; and each $c(x)$ is the biggest path-connected set containing x.

$c(x)$ is path-connected, hence by Proposition 2.5.3 it is connected and then we have the relation

$$c(x) \subseteq C(x)$$

where $C(x)$ is the connected component of x. The path-connected components are not necessarily closed sets. For example if we consider the topologist's sine curve there are two path-connected components, one of them closed and the other not:



2.5.2 Local (path-)connectedness

Definition 2.5.8. A topological space (X, τ_X) is *locally (path-)connected* if for all $x \in X$ there exist a basis of (path-)connected neighborhoods.

Recall that path-connectedness implies connectedness, so:

Proposition 2.5.9. *Local path-connectedness implies local connectedness.*

Now let us study some examples, showing that the previous concepts need not be related.

Examples 2.5.10. (1) $(\mathbb{R}, \tau_u)$ is path-connected and also locally path-connected.

(2) $(0,1) \cup (1,2)$ is not connected, neither path-connected but it is locally path-connected.

(3) (X, τ_{dis}) with X with more than one element is locally path-connected but it is not connected.

(4) The topologist's sine curve, the comb space and the broom space are not locally connected, although they are connected.

(5) $(\{\frac{1}{n} \mid n \in \mathbb{N}\} \cup \{0\}, \tau_u)$ is not a discrete space, but since in any neighborhood of 0 there must be infinitely many elements, the neighborhood is not going to be connected. Hence this space is not locally connected and neither connected.

Theorem 2.5.11. *Let (X, τ_X) be a topological space. Then it is locally connected if and only if the connected components of any open subset are open.*

Proof. In order to prove the *only if* implication let any $U \in \tau$ and $x \in U$. Consider $C_U(x)$ the connected component of x in U and take $y \in C_U(x)$. Since (X, τ_X) is locally connected and U is an open neighbourhood of y, there exists a connected neighborhood $V \subseteq U$ of y, so by definition of connected component and since they form a partition we have

$$y \in V \subseteq C_U(y) = C_U(x).$$

Then $C_U(x)$ is an open set.

To prove the *if* implication take any $x \in X$. For any open subset U containing x $C_U(x)$ is open, so it is a neighbourhood of x. Then

$$\mathcal{B}_x = \{C_U(x) \mid U \in \tau \text{ and } x \in U\}$$

is a connected neighbourhood basis. □

Proposition 2.5.12. *If (X, τ_X) is connected and locally path-connected then it is path-connected.*

Proof. Let $x_0 \in X$ and define

$$H = \{x \in X \mid \text{there exist a path from } x_0 \text{ to } x\}.$$

i. We can always consider the trivial path, then $x_0 \in H$ and so $H \neq \varnothing$.

ii. H is open: Take $x \in H$. Since X is locally path-connected there exists a path-connected neighborhood B of x. For all $y \in B$, there exists a path that connects x and y and since $x \in H$, there also exists a path that connects x and x_0. Thus, we can do the composition of these two paths getting a path from x_0 to y. Therefore $y \in H$, so $B \subseteq H$, and H is open.

ii. H is closed: Let $x \in \overline{H}$. Then for all basic neighborhoods N of x we have $N \cap H \neq \varnothing$, but since X is locally path-connected we can take a path-connected neighborhood B of x such that $B \cap H \neq \varnothing$. Take $y \in B \cap H$, then since $y \in B$ there exists a path between y and x and since $y \in H$ there exists a path between y and x_0 so we can compose this two paths getting a path from x_0 to x, so $x \in H$ and therefore H is closed.

Now since X is connected it does not have proper non-empty subsets which are open and closed at the same time, so $H = X$. Therefore X is path-connected. $\square$

Chapter 3

Axioms of countability

Notation. During this chapter, we will denote $(x_n)_{n\in\mathbb{N}}$ sequences in topological spaces. Besides, we will use the notation $\mathcal{N}_x$ for the neighborhood system of the point x and $\mathcal{B}_x$ for a local base.

3.1 Motivation

After the first year of elementary Calculus, everyone perceives the strength of the sequences to solve many kind of problems in real spaces. For instance, sequences allow us to characterize very important properties such as compactness in $\mathbb{R}^n$ or continuity of mappings from $\mathbb{R}^n$ to $\mathbb{R}^m$ (with the usual topology). More specifically, for continuity we have the following result:

Theorem 3.1.1. *Let $f\colon (\mathbb{R}^n, \tau_u) \to (\mathbb{R}^m, \tau_u)$ be a map. Then f is continuous if and only if for any sequence $(x_n)_{n\in\mathbb{N}} \subset \mathbb{R}^n$ that converges to x, the sequence $(f(x_n))_{n\in\mathbb{N}} \subset \mathbb{R}^m$ converges to $f(x)$.*

If we want to study how much information can sequences give us in more general topological spaces or the minimum conditions needed to generalize the theorems we already know for $\mathbb{R}^n$ it is worth recalling the definition of sequence and convergence of sequences in a general topological space:

Definition 3.1.2. A *sequence* in $X \neq \varnothing$ is a map $f\colon \mathbb{N} \to X$. We shall denote the sequences with the notation introduced at the beginning, where $f(n) = x_n$ is called *general term* of the sequence and $f(\mathbb{N})$ is the *range*.
If τ is a topology over X, we say that a sequence $(x_n)_{n\in\mathbb{N}} \subset X$ *converges* to x in (X, τ) when for all $N \in \mathcal{N}_x$ there exists $n_N \in \mathbb{N}$ such that for every $n \geq n_N$ we have $x_n \in N$. This will be denoted by $(x_n)_{n\in\mathbb{N}} \to x$. (Note that we could also have used basic neighborhoods in the definition). In this case we say that x is a *limit* of the sequence.
Finally, a *subsequence* $\{y_n\}_{n\in\mathbb{N}}$ of the original sequence $(x_n)_{n\in\mathbb{N}}$ is another sequence given by $y_n = x_{\phi(n)}$, where $\phi\colon \mathbb{N} \to \mathbb{N}$ is a strictly increasing function. Subsequences are usually denoted $\{x_{n_k}\}_{k\in\mathbb{N}}$, where we understand $n_k = \phi(k)$.

Unfortunately, the sequences in general topological spaces do not always work satisfactorily, some undesired patologies arise even in very simple cases:

- In general, it is not ensured the uniqueness of the limit. For example, in $(\mathbb{R}, \tau_{Kol})$ the sequence $\{\frac{1}{n}\}_{n\in\mathbb{N}}$ converges to any point less or equal than 0. Indeed, if $a \leq 0$, then every neighborhood of a includes a set of the form $(a - \varepsilon, +\infty)$, so it includes the whole sequence. However, the uniqueness is clearly ensured for Hausdorff spaces (T_2), because if $x \neq y$ we may choose disjoint open neightbourhoods containing each of the points, so it is impossible for both of them to fulfil the condition of containing all the points of the range whose index is greater than some natural number.

- Let's see that Theorem 3.1.1 is not true in general maps for between arbitrary topological spaces. Consider the map $1_{\mathbb{R}} \colon (\mathbb{R}, \tau_{coc}) \to (\mathbb{R}, \tau_u)$. It is not continuous, because there are plenty open sets in τ_u that are not open in τ_{coc} (for instance, any bounded open interval). However, it is not difficult to show that it satisfies the condition of Theorem 3.1.1: if $(x_n)_{n\in\mathbb{N}} \to x$ in $(\mathbb{R}, \tau_{coc})$, consider the set
$$U = (\mathbb{R} - \{x_n \mid n \in \mathbb{N}\}) \cup \{x\} \in \mathcal{N}_x.$$
Then there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ we have $x_n \in U$, which means that $x_n = x$ (recall that we have substracted the range of the sequence from U except for, at most, the point x) and the sequence is semiconstant. Therefore, $(1_{\mathbb{R}}(x_n))_{n\in\mathbb{N}} = (x_n)_{n\in\mathbb{N}}$ converges in $(\mathbb{R}, \tau_u)$ to $x = 1_{\mathbb{R}}(x)$, so the condition holds, although the map is not continuous.

At this point, it is natural to ask ourselves what do we exactly need to characterize continuity just using sequences. In order to find the answer, we will study the case of maps between metrizable topological spaces. From now on, we will use d's as subindexes for topologies to denote metrizable spaces. First, we will need a lemma to prove the generalization of Theorem 3.1.1. In fact, the proof of the lemma contains the fundamental ingredients to cook the best generalization.

Lemma 3.1.3. *Let (X, τ_d) be a metrizable space and $A \subset X$. Then $x \in \overline{A}$ if and only if there exists $(x_n)_{n\in\mathbb{N}} \subset A$ that converges to x.*

Proof. $\Rightarrow$) Let x be a point of $\overline{A}$. Consider the following local base of x:
$$\mathcal{B}_x = \{B(x, \varepsilon) \mid \varepsilon > 0\}$$
We will construct the desired sequence using balls of small radius. By hypothesis, we have that $B(x, \frac{1}{n}) \cap A \neq \varnothing$ for all $n \in \mathbb{N}$. Thus, we can take $x_n \in B(x, \frac{1}{n}) \cap A$ and construct in this way a sequence $(x_n)_{n\in\mathbb{N}} \subset A$. Now, given $\varepsilon > 0$, by the archimedean property of natural numbers we know that exists $n_0 \in \mathbb{N}$ such that $\frac{1}{n_0} < \varepsilon$. Thus, for all $n \geq n_0$ we have that $\frac{1}{n} \leq \frac{1}{n_0} < \varepsilon$, so $x_n \in B(x, \frac{1}{n}) \subset B(x, \varepsilon)$, which proves that given an arbitrary basic neighborhood of x almost all the points of the sequence lay inside it, so the sequence

converges to x.

$\Leftarrow$) Suppose that exists a sequence $(x_n)_{n\in\mathbb{N}}$ that converges to x. Take $N \in \mathcal{N}_x$. Then there exists $n_0 \in \mathbb{N}$ such that $x_n \in N$ for all $n \geq n_0$, which implies that $N \cap A \neq \varnothing$. Since N was an arbitrary neighborhood, we conclude that $x \in \overline{A}$. $\square$

Remark. Point that for the implication $\Leftarrow$) we haven't used that our topological space is metrizable. In fact, that direction is true for an arbitrary topological space. However, in the other implication we have used the balls to construct the sequence, but the essential thing is having a countable number of neighborhoods (that form a local base). We shall discuss this in more detail later, because there is the key.

Now, let's prove the generalization of Theorem 3.1.1 for metric spaces:

Theorem 3.1.4. *Let $f\colon (X,\tau_d) \to (Y,\tau_{d'})$ be a map between two metrizable topological spaces. Then f is continuous if and only if for any sequence $(x_n)_{n\in\mathbb{N}} \subset X$ that converges to x, the sequence $(f(x_n))_{n\in\mathbb{N}} \subset Y$ converges to $f(x)$.*

Proof. $\Rightarrow$) Suppose that f is continuous and $(x_n)_{n\in\mathbb{N}}$ converges to x in (X,τ_d). Let's see that $(f(x_n))_{n\in\mathbb{N}}$ converges to $f(x)$. Take $N \in \mathcal{N}_{f(x)}$. Since f is continuous, we have $f^{-1}(N) \in \mathcal{N}_x$, so there exists $n_0 \in \mathbb{N}$ such that

$$\forall n \geq n_0,\ x_n \in f^{-1}(N) \iff f(x_n) \in N \in \mathcal{N}_{f(x)},$$

so $(f(x_n))_{n\in\mathbb{N}}$ converges to $f(x)$.

$\Leftarrow$) In order to proof continuity, we shall see that for any $A \subset X$ we have $f(\overline{A}) \subset \overline{f(A)}$. The case $A = \varnothing$ is trivial, because $f(\overline{\varnothing}) = \varnothing \subset \overline{f(\varnothing)}$, so we can suppose that A is non-empty. Let $x \in \overline{A}$. By the previous lemma there exists $(x_n)_{n\in\mathbb{N}} \subset A$ that converges to x. Thus, by the hypothesis, $(f(x_n))_{n\in\mathbb{N}} \subset f(A)$ converges to $f(x)$ in (Y,τ_d') and, by the lemma again, $f(x) \in \overline{f(A)}$. Therefore, $f(\overline{A}) \subset \overline{f(A)}$. $\square$

Remark. Point that for $\Leftarrow$) we have needed the lemma, but we haven't used it for the other implication, so that direction is true in arbitrary topological spaces.

3.2 First axiom of countability

As we have said in the remark of Lemma 3.1.3, in order to prove it we only need a countable decreasing local base for each point. Once we have the lemma, it is clear that the corresponding characterization of the continuity holds. This motivates the following definition:

Definition 3.2.1. We say that a topological space (X,τ) *verifies the first axiom of countability*, or simply that is C_I (or *first-countable*) if for every point $x \in X$ there exists a countable local base $\mathcal{B}_x = \{B_n \mid n \in \mathbb{N}\}$.

At first sight, one may think that it is not enough to ensure the lemma, because we do not specify anything about decreasing local neighborhoods. However, the existence of a decreasing countable local base comes for free, because given $\mathcal{B}_x = \{B_n \mid n \in \mathbb{N}\}$ we can construct one very easily. Indeed, take $\mathcal{B}'_x = \{B'_n \mid n \in \mathbb{N}\}$, where

$$\begin{aligned} B'_1 &= B_1 \\ B'_2 &= B_1 \cap B_2 \\ &\vdots \\ B'_n &= B_1 \cap \ldots \cap B_n \end{aligned}$$

Then $\mathcal{B}'_x$ is a decreasing local base for x. Moreover, we can force it to have only open neighborhoods, just taking the interiors of the basic neighborhoods.

Therefore, in C_I spaces the conclusion of Lemma 3.1.3 also holds and we can characterize continuity using sequences as follows:

Theorem 3.2.2. *Let (X, τ) and (Y, τ') be topological spaces with (X, τ) first-countable and $f : (X, \tau) \to (Y, \tau')$ a map between them. Then f is continuous if and only if for any sequence $(x_n)_{n\in\mathbb{N}} \subset X$ that converges to x, the sequence $(f(x_n))_{n\in\mathbb{N}} \subset Y$ converges to $f(x)$.*

Proof. As we have said in the remark after Theorem 3.1.4, sufficiency always holds, so we only need to prove necessity. But the proof is exactly the same of Theorem 3.1.4. Indeed, take $A \subset X$ and $x \in \overline{A}$. By Lemma 3.1.3 we know that there exists $(x_n)_{n\in\mathbb{N}} \subset A$ that converges to x. Thus, by the hypothesis, $(f(x_n))_{n\in\mathbb{N}} \subset f(A)$ converges to $f(x)$ in (Y, τ'_d) and, by the lemma again, $f(x) \in \overline{f(A)}$. Therefore, $f(\overline{A}) \subset \overline{f(A)}$ and f is continuous. □

With this we have reached the best generalization of Theorem 3.1.1 to abstract topological spaces. Point that we don't require the second space to be C_I, because in the second use of the lemma during the proof we only need the implication $\Leftarrow$), which is true in any topological space according to the remark after Lemma 3.1.3. We end up this section studying whether some of the most common topological spaces are C_I or not.

Examples 3.2.3. (1) Given (X, τ_d) we can choose $\mathcal{B}_x = \{B(x, \frac{1}{n}) \subset X \mid n \in \mathbb{N}\}$. This shows in particular that metrizable implies C_I. Therefore, if a given space is not first-countable, it cannot be metrizable.

In (X, τ_{dis}), we can always choose $\mathcal{B}_x = \{\{x\}\}$, so discrete spaces are always C_I.

(2) The case of (X, τ_{ind}) is even simpler than the previous one, because for any point we only have to choose $\mathcal{B}_x = \{X\}$, so indiscrete spaces are always first-countable. Since they are not metrizable, this shows that C_I does not imply metrizability, so the above theorem is really a generalization, not only another way to write the same thing.

(3) Consider $(\mathbb{R}, \tau_{Kol})$. Given $x \in \mathbb{R}$ we can choose $\mathcal{B}_x = \{(x - \frac{1}{n}, +\infty) \mid n \in \mathbb{N}\}$ as countable local base, so this space also verifies the firts axiom of countability.

(4) Consider $(\mathbb{R}, \tau_{Sor})$. Given $x \in \mathbb{R}$ a posible countable local base is $\mathcal{B}_x = \{[x, x + \frac{1}{n}) \mid n \in \mathbb{N}\}$, so this space is also C_I.

(5) What about $(\mathbb{R}, \tau_{cof})$? It turns out that it is not C_I. Indeed, take $x \in \mathbb{R}$ and, by contradiction, suppose that exists $\mathcal{B}_x = \{B_n \mid n \in \mathbb{N}\}$ open countable local base. Then by the De Morgan laws we have

$$\left(\bigcap_{n\in\mathbb{N}} B_n\right)^c = \bigcup_{n\in\mathbb{N}} B_n^c.$$

Since a countable union of finite sets is countable, it cannot be the whole $\mathbb{R}$ (it isn't countable), we deduce that there are infinitely many points in the intersection of the basic neighborhoods of x. Take $y \neq x$ in the intersection and consider the set $A = \mathbb{R} \setminus \{y\}$, which is clearly an open neighborhood of x. However, it doesn't contain the point y, which is contained in every set of $\mathcal{B}_x$, so we can conclude that there does not exist $B_j \in \mathcal{B}_x$ such that $B_j \subset A$, in contradiction with the hypothesis that $\mathcal{B}_x$ is a local base. Therefore, the space is not C_I. A similar argument is valid for $(\mathbb{R}, \tau_{coc})$, taking into account that $\mathbb{R}$ cannot be obtained as a numerable union of countable sets.

3.3 Second axiom of countability

Of course, at this juncture the sharp reader suspects that if the previous section was devoted to the *first* axiom of countability, there must be at least a *second* one. As we shall see, it is stronger than the previous one, and is in fact as important as the other one due to two major reasons:

- A lot of very well known topological spaces verify it, in particular $(\mathbb{R}, \tau_u)$.
- It is a crucial condition in many metrizability theorems (results concerning conditions to ensure or discard metrizability).

Definition 3.3.1. We say that a topological space (X, τ) *verifies the second axiom of countability*, or simply that is C_{II} (or *second-countable*) if it admits a countable base.

It is straighfoward to verify that C_{II} implies C_I, because given a countable base β and a point x, a posible local base is $\mathcal{B}_x = \{B \in \beta \mid x \in B\}$. Let's study some of the most common topological spaces.

Examples 3.3.2.

(1) In $(\mathbb{R}, \tau_u)$ the set $\beta = \{(a, b) \subset \mathbb{R} \mid a < b \; a, b \in \mathbb{Q}\}$ is a countable base, since $\#\beta \leq \#(\mathbb{Q} \times \mathbb{Q}) = \#\mathbb{N}$.

(2) Following the previous example, something similar happens in greater dimensions. In $(\mathbb{R}^n, \tau_u)$ the set $\beta = \{B(x, \frac{1}{n}) \subset \mathbb{R}^n \mid x \in \mathbb{Q}^n \; n \in \mathbb{N}\}$ is a countable base.

(3) In the case of $(\mathbb{R}, \tau_{Kol})$ a possible countable base is $\beta = \{(a, +\infty) \mid a \in \mathbb{Q}\}$.

(4) Indiscrete spaces are always C_{II}, since any topology is in particular a base for itself, and indiscrete topologies have always finite cardinal and so, countable. This shows in particular that C_{II} does not imply metrizability.

(5) If X is not countable, then (X, τ_{dis}) is not second-countable, because any base must contain all the singletons. This shows that metrizability does not imply C_{II}.

(6) $(\mathbb{R}, \tau_{Sor})$ may seem to be second countable at first sight, choosing as base $\beta = \{[a, b) \mid a < b \ a, b \in \mathbb{Q}\}$. However it turns out that there does not exist $B \in \beta$ such that $\sqrt{2} \in B \subset [\sqrt{2}, 3)$, because all the "basic opens" of β containing $\sqrt{2}$ are of the form $[a, b)$ for some $a < \sqrt{2}$ (the inequality is strict). Of course, this is not enough to show that our space is not C_{II}, but it is not too difficult. Let β be an arbitrary base and choose $x, y \in \mathbb{R}$ distinct. Consider the open sets $U = [x, x+1)$ and $V = [y, y+1)$. By the definition of base we have

$$\exists B_x \in \beta \text{ such that } x \in B_x \subset [x, x+1)$$
$$\exists B_y \in \beta \text{ such that } y \in B_y \subset [y, y+1).$$

Since the infimum of B_x and B_y is not the same (x and y respectively), they must be different sets, so any base β has at least the cardinal of the continuum.

To finish this section, we will show that the behaviour of the two axioms of countability presented is quite stable:

Proposition 3.3.3. *The properties C_I and C_{II} are hereditary, productive (for finite and numerable products) and topological.*

Proof. Supose that (X, τ) is C_{II} and $A \subset X$. If $\beta_X = \{B_n \in \tau \mid n \in \mathbb{N}\}$ is a countable local base of (X, τ), it is clear that $\beta_A = \{B_n \cap A \in \tau_A \mid n \in \mathbb{N}\}$ is a countable local base for (A, τ_A). Similarly, if (X, τ) is C_I and $x \in X \cap A$, given a countable local base $\mathcal{B}_x^X = \{B_n \in \tau \mid n \in \mathbb{N}\}$ in (X, τ), we can construct another one in the subspace just taking $\mathcal{B}_x^A = \{B_n \cap A \in \tau_A \mid n \in \mathbb{N}\}$.

To see that those properties are preserved under finite products, the idea is also very simple. If (X, τ_X) and (Y, τ_X) are both C_{II} and β_X, β_Y denote two countable bases respectively, we can clearly choose as a base for the product topology de set

$$\beta = \beta_X \times \beta_Y = \{B_X \times B_Y \mid B_X \in \beta_x,\ B_Y \in \beta_Y\},$$

which is clearly countable, because the cartesian product of countable sets is also countable. A trivial induction generalizes this to finite products.
However, for the case of numerable products, everything becomes more difficult. If (X_n, τ_n) are C_{II} spaces, the base of the product is given by

$$\beta_{Tych} = \Big\{ \bigcap_{j \in J} \pi_j^{-1}(U_j) \mid J \subset \mathbb{N} \text{ finite}, U_j \in \tau_j \Big\}.$$

Let's denote β_n a countable base of the space (X_n, τ_n) and $\phi_n\colon \beta_n \to \mathbb{N}$ a bijective map. Then another possible base for the product is

$$\beta'_{Tych} = \Big\{ \bigcap_{j\in J} \pi_j^{-1}(B_j) \mid J \subset \mathbb{N} \text{ finite}, \ B_j \in \beta_j \Big\}.$$

Indeed, if $U_i \in \tau_i$ we have $x = (x_1, x_2, \dots) \in \pi_i^{-1}(U_i) \iff x_i \in U_i$. So there exists $B_i \in \beta_i$ such that $x_i \in B_i \subset U_i \Rightarrow x \in \pi_i^{-1}(B_i) \subset \pi_i^{-1}(U_i)$. This can trivially be extended to finite products, so, β'_{Tych} is a basis. But it is not clear at all that it is countable. In order to show it, point that the basic opens of β'_{Tych} are of the form

$$B_1 \times B_2 \times \cdots \times B_n \times \cdots$$

where $B_i = X_i$ for *almost all* i (except a finite number of them). The other factors are, of course, basic open sets of the corresponding bases. This allows us to obtain β'_{Tych} as a numerable disjoint union of numerable sets, considering separately the products depending on the number of factors that are not the whole space. For each $n \in \mathbb{N}$, denote $\beta_n \subset \beta'_{Tych}$ the set containing those basic opens that only have n factors that are not the whole space. Then

$$\beta'_{Tych} = \dot{\bigcup_{n\in\mathbb{N}}} \beta_n,$$

so it is enough to show that each β_n is countable. We don't really need to be tactful, so we will construct an injective mapping from β_n to $\mathbb{N}^{2n}$, which is countable for all $n \in \mathbb{N}$. Define the map $f\colon \beta_n \to \mathbb{N}^{2n}$ by

$$f(X_1 \times \cdots \times B_{i_1} \times \cdots \times B_{i_n} \times \cdots) = (i_1, \phi_{i_1}(B_{i_1}), \dots, i_n, \phi_{i_n}(B_{i_n}))$$

where $i_1 < i_2 < \cdots < i_n$ are natural numbers. The injectivity of the map follows from the fact that two sets with same image through f must have the basic opens in the same positions (otherwise the images would be different in the position of the indexes), but in that case the bijectivity of the ϕ_i maps forces the equality of sets. Thus, each β_n is countable, so β'_{Tych} also. For the C_I case the idea is exactly the same in the finite and infinite case, considering in this last case local bases of the form

$$\mathcal{B}_x = \Big\{ \bigcap_{j\in J} \pi_j^{-1}(B_j) \mid J \subset \mathbb{N} \text{ finite}, \ B_j \in \mathcal{B}_{x_i} \Big\},$$

where $x = (x_1, x_2, \dots)$ and $\mathcal{B}_{x_i}$ is a local base of x_i in X_i.

Finally, to see that those properties are topological, just point that if (X, τ_X) and (Y, τ_Y) are homeomorphic and β_X is a base of the first space, then $\beta_Y = \{h(B) \in \tau_Y \mid B \in \beta_X\}$ is a base of the second one (h is of course a homeomorphism). Something similar happens with local bases, because given $y \in Y$, a possible local base is $\mathcal{B}_y^Y = \{h(B) \in \mathcal{N}_y^Y \mid B \in \mathcal{B}_x^X\}$, where $y = h(x)$ (recall that such x exists and is unique due to the bijectivity) and $\mathcal{B}_x^X \subset \mathcal{N}_x^X$ is a local base of x in the first space. $\square$

3.4 Third and fourth axioms of countability. Separability and metrizability theorems

Although they are thought to be less important than the first two ones, there are another two properties considered axioms of countability: separability and Lindelöf property. Their main use is giving metrizability conditions.

Definition 3.4.1. We say that a topological space (X, τ) is *separable* when there exists $D \subset X$ dense and countable.

Definition 3.4.2. A topological space (X, τ) owns the *Lindelöf property* or is a *Lindelöf space* when every open cover of X admits a countable subcover. In particular, compact spaces are always Lindelöf spaces.

Let's show that the second axiom of countability is stronger than the third and the fourth ones:

Proposition 3.4.3. *Let (X, τ) be a C_{II} space. Then it is separable and Lindelöf.*

Proof. Let $\beta = \{B_n \in \tau \mid n \in \mathbb{N}\}$ be a countable base. Let's start proving separability. For all $n \in \mathbb{N}$ choose $x_n \in B_n$ and define de set $D = \{x_n \mid n \in \mathbb{N}\}$. It is clearly countable and dense, because it is defined to have nonempty intersection with all the sets of the base β. Therefore, the space is separable.

In order to prove that it is a Lindelöf space, let $\{U_i\}_{i\in I}$ an open cover of X. For each basic open B_n let V_n be any U_i that includes it. If such U_i doesn't exist, pick as V_n any set of the cover randomly. We claim that $\{V_n\}_{n\in\mathbb{N}}$ covers the whole space. Indeed, suppose by contradiction that exists $x \in X$ not contained in any V_n. Since $\{U_i\}_{i\in I}$ covers X, there exists $j \in I$ such that $x \in U_j$. Therefore, we can find a basic open B_k such that $x \in B_k \subset U_j$. Thus, we have that B_k is included in some set of the initial cover, so B_k is included in V_k and therefore contains the element x, contradiction. Since $\{V_n\}_{n\in\mathbb{N}}$ is a countable subcover, it follows that (X, τ) is a Lindelöf space. □

The converse is not true in general, but it can be proved that in metrizable spaces *those three properties are equivalent*, so this gives us a method to show that certain topological spaces are not metrizable.

Examples 3.4.4. (1) We have already seen that $(\mathbb{R}, \tau_{Sor})$ is not second-countable, but it is clearly separable, because the set $\mathbb{Q}$ intersects any basic open set (any interval of the form $[x, x + \varepsilon)$ must contain rational points). Consequently, $(\mathbb{R}, \tau_{Sor})$ is not metrizable.

(2) The real line with the scattered topology

$$(\mathbb{R}, \tau_{sca} = \{U \subset \mathbb{R} \mid U = V \cup S,\ B \in \tau_u,\ S \subset \mathbb{I}\})$$

is not second-countable, because any base must contain a singleton for each irrational point. However, it can be showed that it is Lindelöf. Indeed, assume that $\{U_i\}_{i\in I} \subset \tau_{sca}$ is an open cover of $\mathbb{R}$. For each rational point q there exists a set of the cover such that $q \in U_{i_q}$. Point that it is only possible if U_{i_q} includes a usual open neighborhood of q, so exists $\varepsilon_q > 0$ such that $(q-\varepsilon_q, q+\varepsilon_q) \subset U_{i_q}$. We may think that $\{U_{i_q}\}_{q\in\mathbb{Q}}$ is a possible subcover, but it is not ensured that all irrational points are inside. However, if we show that $A = \mathbb{R} - \bigcup_{q\in\mathbb{Q}} U_{i_q}$ is countable we could obtain a complete subcover adding a countable number of sets of the original cover, so we would be done. It is enough to show that $B = \mathbb{R} - \bigcup_{q\in\mathbb{Q}}(q-\varepsilon_q, q+\varepsilon_q)$ is countable, because $A \subset B \subset \mathbb{I}$.

By contradiction, suppose that B is not countable. Then

$$\mathbb{R} - B = \bigcup_{q\in Q}(q-\varepsilon_q, q+\varepsilon_q)$$

is open in the usual topology, so it can be obtained as numerable disjoint union of open intervals in a unique way. Nevertheless, for each point $b \in B$ there must be an interval of the form $(b, b+\varepsilon_b)$ (recall that $B \subset \mathbb{I}$, which implies that there are not intervals included in B), so the number of intervals is uncountable, contradiction. This shows that B and A are countable. Therefore, the scattered line is not metrizable, because it is Lindelöf but not C_{II}.

However, rather than having *necessity conditions* for metrizability, we may be interested in theorems that give *sufficiency or equivalence conditions* to ensure it. Unfortunately, proving those kind of results is far from the scope of the course, so we will just introduce some of the so called *axioms of separability* and state without proof two important results due to Urysohn.

Definition 3.4.5. We say that a topological space (X,τ) is *regular* when every non-empty closed subset C of X and a point x not contained in C can be separated by two disjoint open sets. Simbolically, given $C \in \mathcal{C}$ and $x \in X \smallsetminus \mathcal{C}$, then there exist $U, V \in \tau$ such that $C \subset U$, $x \in V$ and $U \cap V = \varnothing$. A T_1 space that is also regular is said to be T_3.

We say that X is *completely regular* if given a non-empty closed set C and a point x not in C there exists a continuous map $f\colon X \to [0,1]$ such that $f(x) = 1$ and $f(C) = \{0\}$. A T_1 space that is also completely regular is said to be $T_{3^1/_2}$.

We say that X is *normal* if given two disjoint closed sets C, D there exist two open sets U, V such that $C \subset U$, $D \subset V$ and $U \cap V = \varnothing$. A T_1 space that is also normal is said to be T_4.

It is pretty clear that complete regularity implies regularity. Indeed, given C closed in X and x not in C let f be a map satisfying the conditions of the definition and choose U, V disjoint open neighborhoods of 0 and 1 respectively. Then $f^{-1}(U)$ is open in X and includes C, $f^{-1}(V)$ is also open and contains the point x and both sets are clearly disjoint. Therefore $T_{3^1/_2}$ implies T_3. Besides, taking into account that a space is T_1 if and only if singletons are closed, regularity and T_1 allow us to separate points using disjoint open sets, so T_3 implies T_2.

Theorem 3.4.6 (Urysohn's lemma)**.** *Let (X,τ) be a normal space and C, D disjoint closed sets. Then there exists a continuous map $f\colon X \to [0,1]$ such that $f(c) = 0$ for all $c \in C$ and $f(d) = 1$ for all $d \in D$.*

This shows in particular that T_4 implies $T_{3^1/_2}$, so we have the following chain of implications:

$$T_4 \implies T_{3^1/_2} \implies T_3 \implies T_2 \implies T_1 \implies T_0$$

It may seem curious a fraction between all those integer indices. Well, the concept of complete regularity was introduced after regularity, normality and the definitions of T_4 and T_3 were stablished, but Urysohn's lemma shows that it is between them. Who knows if it was a joke, but someone suggested a rational index and nowadays is a quite common denomination. There exist more axioms of separability, always listed in order increasing strength, but we will stop here the rain of T_i's.

Theorem 3.4.7 (Urysohn's metrizability theorem)**.** *Let (X, τ) be a C_{II} and T_3 topological space. Then it is metrizable.*

Chapter 4

Complete metric spaces

Notation. Even though the topology is always behind the ideas that follow, during this chapter we will develop the theory focusing more on distances, which we shall denote using d's. Therefore, whenever we talk about purely topological concepts in metric spaces they should be understood for the topological space induced by the metric.

4.1 Introduction

As we have seen in the previous chapter, there are many concepts of elementary Calculus that can be studied from a more general point of view. Notions as continuity, sequences and convergence have their analogue in general topological spaces. Nevertheless, talking about Cauchy sequences or uniform continuity in general topological spaces does not make sense, they are not provided with enough resources to extend the original idea to them.

Fortunately, it's not all bad news, because those concepts are easily defined in metric spaces and that will allow us to obtain very nice results concerning metrizable spaces. In fact, there exists a more general type of topological spaces in which we can consistently define Cauchy sequences and uniform continuity, namely uniform spaces. However, we will restrict our study to metric spaces.

Definition 4.1.1. Let (X, d) be a metric space. We say that a sequence $(x_n)_{n\in\mathbb{N}} \subset X$ is a *Cauchy sequence* if for all $\varepsilon > 0$ there exists a natural number n_0 such that when $n, m \geq n_0$ then we have $d(x_n, x_m) < \varepsilon$.

It is clear from the definition that the property of being a Cauchy sequence does not depend on the space itself, but on the distance. More precisely, if (X, d) is a metric space, $A \subset X$ and $(x_n)_{n\in\mathbb{N}} \subset A$, then $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in (X, d) if and only if it is a Cauchy sequence in (A, d_A), where d_A is the restriction of the distance to A.

As the reader knows, in $\mathbb{R}^n$ with the usual distance Cauchy sequences always converge. Unfortunately, this is not true in general metric spaces.

Example 4.1.2. Consider the metric space $((0,+\infty), d_u)$. The sequence $\{\frac{1}{n}\}_{n\in\mathbb{N}}$ is a Cauchy sequence there, because so is in $(\mathbb{R}, d_u)$. However, the unique possible limit is zero, that is not in $(0,+\infty)$. Therefore, the sequence is not convergent in $((0,+\infty), d_u)$ (in spite of the fact that it is convergent in $(\mathbb{R}, d_u)$).

In general, we need more than being Cauchy to ensure the convergence of a sequence, as shows the following

Proposition 4.1.3. *Let (X,d) be a metric space and $(x_n)_{n\in\mathbb{N}}$ a sequence in X. The sequence $(x_n)_{n\in\mathbb{N}}$ is convergent if and only if it is Cauchy and has a convergent subsequence $\{x_{n_k}\}_{k\in\mathbb{N}}$.*

Proof. Let us start proving sufficiency. Suppose that $(x_n)_{n\in\mathbb{N}}$ converges to x. Then given $\varepsilon > 0$ consider the number $\frac{\varepsilon}{2} = \varepsilon'$. By definition of convergence, exists a natural number n_0 such that whenever $n > n_0$ we have $d(x_n, x) < \varepsilon'$. Therefore, if $m > n_0$ we have

$$d(x_n, x_m) \leq d(x_n, x) + d(x, x_m) < 2 \cdot \varepsilon' = \varepsilon,$$

so $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence. Finally, taking into account that the whole sequence is in particular a subsequence that converges by hypothesis, the result follows.

To prove necessity assume that $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence that has a subsequence $\{x_{n_k}\}_{k\in\mathbb{N}}$ that converges to x. Given $\varepsilon > 0$ consider the number $\frac{\varepsilon}{2} = \varepsilon'$. On the one hand, exists n_0 such that when $n, m > n_0$ we have $d(x_n, x_m) < \varepsilon'$. On the other hand, exists k_0 such that whenever $k > k_0$ if follows that $d(x_{n_k}, x) < \varepsilon'$. Now, we can consider $k \in \mathbb{N}$ satisfying $n_k > \max\{n_0, n_{k_0}\}$. Therefore, if $n > n_k$ we have

$$d(x_n, x) \leq d(x_n, x_{n_k}) + d(x_{n_k}, x) \leq 2 \cdot \varepsilon' < \varepsilon,$$

so the original sequence also converges to x. $\square$

Normally, it is not trivial determining whether a sequence has a convergent subsequence, so we may be interested in metric spaces in which "being Cauchy" and "being convergent" is equivalent. This allows us to ensure the convergence of a sequence just checking if it is Cauchy, which is many times easier than checking convergence, because we do not need to know the limit. This motivates the following:

Definition 4.1.4. We say that a metric space (X,d) is *complete* if every $(x_n)_{n\in\mathbb{N}} \subset X$ that is Cauchy is also convergent in (X,d).

Examples 4.1.5. Let's see a few simple examples:

(1) As seen in elementary Calculus and mentioned before, $(\mathbb{R}^n, d_u)$ is complete.

(2) (X, d_{dis}) is always complete. Indeed, suppose that $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence and take $0 < \varepsilon < 1$. It turns out that $d_{dis}(x_n, x_m) < \varepsilon$ if and only if $x_n = x_m$. This together with the fact that the it is Cauchy allows us to conclude that $(x_n)_{n\in\mathbb{N}}$ is semiconstant, and so convergent.

(3) According to Example 4.1.2, the metric space $((0, +\infty), d_u)$ is not complete.

We will finish this section defining the concept of uniform continuity and showing a basic result that also concerns Cauchy sequences. As the reader shall see, the proof is very similar to the usual one in $\mathbb{R}^n$.

Definition 4.1.6. A map between metric spaces $f\colon (X, d) \longrightarrow (Y, d')$ is said to be *uniformly continuous* if for all $\varepsilon > 0$ exists $\delta > 0$ such that $d(x_1, x_2) < \delta$ implies $d'(f(x_1), f(x_2)) < \varepsilon$.

Proposition 4.1.7. *Let $f\colon (X, d) \longrightarrow (Y, d')$ be a uniformly continuous map between metric spaces and $(x_n)_{n\in\mathbb{N}}$ a Cauchy sequence in (X, d). Then $(f(x_n))_{n\in\mathbb{N}}$ is a Cauchy sequence in (Y, d').*

Proof. Take $\varepsilon > 0$. By definition of uniform continuity there exists $\delta > 0$ such that $d(x_1, x_2) < \delta$ implies that $d'(f(x_1), f(x_2)) < \varepsilon$. Besides, by definition of Cauchy sequence we know that for that δ there exists a natural number n_0 such that when $n, m \geq n_0$ we have $d(x_n, x_m) < \delta$, so $d'(f(x_n), f(x_m)) < \varepsilon$. Therefore, given a positive number ε we have been able to find a natural n_0 satisfying the definition, which implies that $(f(x_n))_{n\in\mathbb{N}}$ is a Cauchy sequence. $\square$

4.2 Completeness and Topology

Let's put on Topology glasses again and recall that in metrizable spaces the definition of convergence in terms of neighborhoods was equivalent to the one based on distances. Hence, Example 4.1.2 shows that completeness is not a hereditary property. However, it is not difficult to show that it is weakly hereditary. Even more, it is only inherited by closed subsets.

Proposition 4.2.1. *Let (X, d) be a complete metric space and $A \subset X$. Then (A, d_A) is complete if and only if A is closed.*

Proof. $\Rightarrow$) Assume that (A, d_A) is complete. Let's show that $\overline{A} = A$. The inclusion $\supset$ always holds, so we only have to prove $\subset$. According to Lemma 3.1.3 $x \in \overline{A}$ if and only if there exists $(x_n)_{n\in\mathbb{N}} \subset A$ that converges to $x \in X$. Thus, $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in (X, d) included in A, which implies that is Cauchy in (A, d_A). Since it is by hypothesis a complete metric space, $(x_n)_{n\in\mathbb{N}}$ converges to $y \in A$, but due to the uniqueness of the limit in Hausdorff spaces we conclude that $y = x \in A$.

$\Leftarrow$) Assume that A is closed and let $(x_n)_{n\in\mathbb{N}}$ be a Cauchy sequence in (A, d_A). Then it is also a Cauchy sequence in (X, d), so converges to a point $x \in X$. According to Lemma 3.1.3 and using that A is closed we have that $x \in \overline{A} = A$. Hence, $(x_n)_{n\in\mathbb{N}}$ converges in (A, d_A) and it is complete. $\square$

But the inconveniences of the behaviour of completeness that are showed by Example 4.1.2 do not end here, because it also proves that completeness is not a topological property. In fact, $(\mathbb{R}, d_u)$ is homeomorphic to $((0, +\infty), d_u)$, but the first one is complete and the second one is not. However, the completeness is preserved by isometries. It is not difficult to show that isometries are uniformly continuous (just take $\varepsilon = \delta$ in the definition) and homeomorphisms (recall that the inverse of an isometry is also an isometry, so the continuity of the inverse is trivial). Therefore, using Theorem 4.1.7 and Theorem 3.1.4 the result follows easily.

Anyways, in metric spaces there is a very close relation between compactness and completeness. In order to show this, we will need to introduce some definitions concerning sequences and compactness and a result that we won't prove. Point that the concepts that follow are defined in general topological spaces, but they are specially useful in metrizable spaces.

Definition 4.2.2. Let (X, τ) be a topological space.

- If every infinite subset of X contains a limit point we say that the space is *limit point compact*.
- If every sequence $(x_n)_{n\in\mathbb{N}}$ has a convergent subsequence we say that the space is *sequentially compact*.

Theorem 4.2.3. *Let (X, d) be a metric space. Then the following are equivalent*:

(i) *X is compact*

(ii) *X is limit point compact.*

(iii) *X is sequentially compact.*

Definition 4.2.4. A metric space (X, d) is said to be *totally bounded* or *precompact* if for every $\varepsilon > 0$ there is a finite cover of X by balls of radius ε.

Clearly, any compact space is also precompact, because $\{B(x, \varepsilon)\}_{x\in X}$ is an open cover of X, so there exists a finite subcover. Now, we are ready to prove the relation between compactness and completeness.

Theorem 4.2.5. *A metric space (X, d) is compact if and only if it is complete and totally bounded.*

Proof. The implication $\Rightarrow$) is quite straightforward. On the one hand, the precompactness is automatically ensured by the compactness. On the other hand, by Theorem 4.2.3 the space is sequentially compact, so in particular every Cauchy sequence has a convergent subsequence. Thus, by Proposition 4.1.3 every Cauchy sequence converges, so the space is complete.

In order to show the implication $\Leftarrow$), due to Theorem 4.2.3 it suffices to prove that a complete totally bounded metric space is also sequentially compact. Given a sequence $(x_n)_{n\in\mathbb{N}}$ construct a subsequence following these steps:

1. Using that the space is totally bounded, cover X by finitely many balls of radius 1. At least one of those balls, say B_1, contains x_n for infinitely many $n \in \mathbb{N}$. Define $J_1 = \{n \in \mathbb{N} \mid x_n \in B_1\}$, the set of indexes of the elements in the sequence contained in B_1.

2. Now, cover X by a finite number of balls of radius $1/2$. Again, at least one of them, say B_2, must contain x_n for infinitely many $n \in J_1$, because J_1 is infinite. Then we can define $J_2 = \{n \in J_1 \mid x_n \in B_2\} \subset J_1$.

3. In general given $J_k \subset J_{k-1}$ infinite we can find a ball B_{k+1} of radius $1/(k+1)$ such that $J_{k+1} = \{n \in J_k \mid x_n \in B_{k+1}\} \subset J_k$ is also infinite. This gives us a set of indexes and a ball of radius $1/k$ for all natural k.

4. Now, pick $n_1 \in J_1$ and for $k \geq 2$ choose $n_k \in J_k$ such that $n_k > n_{k-1}$. Point that every J_k is infinite, so we can always find such n_k contained there. In this way we construct a subsequence $\{x_{n_k}\}_{k\in\mathbb{N}}$.

Finally, let's show that $\{x_{n_k}\}_{k\in\mathbb{N}}$ is a Cauchy sequence (and convergent due to completeness). Given a positive number ε choose $k_0 \in \mathbb{N}$ such that $2/k_0 < \varepsilon$. Since $J_1 \supset J_2 \supset \ldots$ for $i, j \geq k_0$ the indices n_i and n_j belong to J_{k_0}, so $x_{n_i}, x_{n_j} \in B_{k_0}$, a ball of radius $1/k_0$. This implies that $d(x_{n_i}, x_{n_j}) < 2/k_0 < \varepsilon$. Thus, the space is sequentially compact. □

To finish this section, we will show that completeness is a productive property for finite products. Before we start, remark that it suffices to show the case of two factors, because a trivial induction allows us to generalize the finite case (it can be proved that the finite product of topological spaces is "associative").

Theorem 4.2.6. *Completeness is a productive property for finite products.*

Proof. The proof of this is quite long, and it will be divided in four steps.

Step 1: Metrizability is finitely productive. Let (X_1, d_1) and (X_2, d_2) be metric spaces and consider the product space $(X_1 \times X_2, \tau_{Tych})$ (using, of course, the topology induced by the metric). Define the map $d\colon X_1 \times X_2 \to \mathbb{R}$ by

$$d(x, y) = \max\{d_1(x_1, y_1), d_2(x_2, y_2)\},$$

where $x = (x_1, x_2)$ and $y = (y_1, y_2)$. Let's show it is a metric on $X_1 \times X_2$:

(1) Since d_1 and d_2 are metrics, if follows that $d \geq 0$. Moreover, we have

$$\begin{aligned} d(x, y) = 0 &\iff \max\{d_1(x_1, y_1), d_2(x_2, y_2)\} = 0 \\ &\iff d_1(x_1, y_1) = d_2(x_2, y_2) = 0 \\ &\iff x_1 = y_1 \wedge x_2 = y_2 \\ &\iff x = y, \end{aligned}$$

so d is positive.

(2) Since $d_i(x_i, y_i) = d_i(y_i, x_i)$ for $i = 1, 2$, it follows that $d(x, y) = d(y, x)$ for all $x, y \in X_1 \times X_2$, so d is symmetric.

(3) Suppose that $z = (z_1, z_2)$. Then

$$\begin{aligned} d(x, y) &= \max\{d_1(x_1, y_1), d_2(x_2, y_2)\} = d_i(x_i, y_i) \leq d_i(x_i, z_i) + d(z_i, y_i) \\ &\leq \max\{d_1(x_1, z_1), d_2(x_2, z_2)\} + \max\{d_1(z_1, y_1), d_2(z_2, y_2)\} \\ &\leq d(x, z) + d(z, y), \end{aligned}$$

so the triangle inequality holds.

Now, if we prove that $\tau_{Tych} = \tau_d$ we would be done. It is enough to show that the set open balls with respect to the distance d, that we will denote β, is a base of τ_{Tych}. On the one hand, given a positive number ε and $x = (x_1, x_2) \in X_1 \times X_2$ we have

$$\begin{aligned} B(x, \varepsilon) &= \{(y_1, y_2) \in X_1 \times X_2 \mid \max\{d_1(x_1, y_1), d_2(x_2, y_2)\} < \varepsilon\} \\ &= \{(y_1, y_2) \in X_1 \times X_2 \mid d_1(x_1, y_1), d_2(x_2, y_2) < \varepsilon\} \\ &= B(x_1, \varepsilon) \times B(x_2, \varepsilon) \in \tau_{Tych}, \end{aligned}$$

so $\beta \subset \tau_{Tych}$. On the other hand, given $U \in \tau_{Tych}$ and $x = (x_1, x_2) \in U$ there exists a set of the form $B(x_1, \varepsilon_1) \times B(x_2, \varepsilon_2)$ included in U, so taking $\varepsilon = \min\{\varepsilon_1, \varepsilon_2\}$ we have

$$x \in B(x, \varepsilon) \subset B(x_1, \varepsilon_1) \times B(x_2, \varepsilon_2) \subset U,$$

which shows that β is in fact a base of τ_{Tych}.

Step 2: A sequence $\{x_k = (x_{k1}, x_{k2})\}_{k \in \mathbb{N}}$ is convergent in $(X_1 \times X_2, d)$ if and only if $\{x_{ki}\}_{k \in N}$ is convergent in (X_i, d_i) for $i = 1, 2$.

To show the implication $\Rightarrow$), assume that $\{x_k = (x_{k1}, x_{k2})\}_{k \in \mathbb{N}}$ converges to $x = (x_1, x_2)$. This means that given $\varepsilon > 0$ there exists $k_0 \in \mathbb{N}$ such that when $k > k_0$ we have

$$\begin{aligned} &d(x_k, x) = \max\{d_1(x_{k1}, x_1), d_2(x_{k2}, x_2)\} < \varepsilon \\ &\iff d_1(x_{k1}, x_1) < \varepsilon \text{ and } d_2(x_{k2}, x_2) < \varepsilon, \end{aligned}$$

so k_0 is a valid number to show that $\{x_{ki}\}_{k \in N}$ converges to x_i.

The implication $\Leftarrow$) is very similar. If $\{x_{ki}\}_{k \in N}$ converges to x_i, given $\varepsilon > 0$ exists k_i natural such that whenever $k > k_i$ we have $d_i(x_{ki}, x_i) < \varepsilon$, for $i = 1, 2$. Thus, if we choose $k_0 = \max\{k_1, k_2\}$ and $k > k_0$ we have

$$\begin{aligned} &d(x_{k1}, x_1) < \varepsilon \wedge d(x_{k2}, x_2) < \varepsilon \\ &\iff \max\{d_1(x_{k1}, x_1), d_2(x_{k2}, x_2)\} = d(x_k, (x_1, x_2)) < \varepsilon, \end{aligned}$$

so $\{x_k = (x_{k1}, x_{k2})\}_{k \in \mathbb{N}}$ converges to (x_1, x_2).

Step 3: A sequence $\{x_k = (x_{k1}, x_{k2})\}_{k\in\mathbb{N}}$ is Cauchy in $(X_1 \times X_2, d)$ if and only if $\{x_{ki}\}_{k\in N}$ is Cauchy in (X_i, d_i) for $i = 1, 2$. The proof is very similar to the one of the previous step. We only have to change a pair of details, so we won't reproduce it completely. Basically, the unique things that we must change are that in this case we choose natural numbers n and m greater than certain $k_0 \in \mathbb{N}$ and later we should have to replace x_{ki} with x_{ni} and x_i with x_{mi} for $i = 1, 2$.

Step 4: Completeness is finitely productive. It is a straight consequence of third and fourth steps. In effect, assume that (X_i, d_i) is complete for $i = 1, 2$ and $\{x_k = (x_{k1}, x_{k2})\}_{k\in\mathbb{N}}$ in $(X_1 \times X_2, d)$ is a Cauchy sequence. By step 3 $\{x_{ki}\}_{k\in N}$ is also a Cauchy sequence in (X_i, d_i) for $i = 1, 2$. Due to completeness in each X_i we deduce that $\{x_{ki}\}_{k\in N}$ converges for $i = 1, 2$, and according to step 2 $\{x_k\}_{k\in\mathbb{N}}$ also converges in $(X_1 \times X_2, d)$, which means that the product space is complete. □

4.3 Completion of metric spaces

As we have seen previously, not all metric spaces are complete. However, a good mathematician can not accept blithely this situation and must (try to) go further in a reasonable way. As we will see in this section, given an abstract metric space we will always be able to construct a *unique* complete metric space *containing* it. Moreover, the new metric space will not be too *big* compared to the old one. Beware the emphasized terms, they must be carefully understood in the context we are working. The proof is long and technical, and we will first need a lemma.

Lemma 4.3.1. *Let (X, d) be a metric space and $\{a_n\}_{n\in\mathbb{N}}$ and $\{b_n\}_{n\in\mathbb{N}}$ two convergent sequences in X. Then*

$$d\big(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\big) = \lim_{n\to\infty} d(a_n, b_n).$$

Proof. It is a consequence of the triangle inequality. On the one have, we have

$$\begin{aligned}\lim_{n\to\infty} d(a_n, b_n) &\leq \lim_{n\to\infty}\big[d\big(a_n, \lim_{n\to\infty} a_n\big) + d\big(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\big) + \big(b_n, \lim_{n\to\infty} b_n\big)\big]\\ &= d\big(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\big).\end{aligned}$$

In a similar way,

$$\begin{aligned}d\big(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\big) &= \lim_{n\to\infty} d\big(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\big)\\ &\leq \lim_{n\to\infty}\big[d\big(\lim_{n\to\infty} a_n, a_n\big) + d(a_n, b_n) + d\big(b_n, \lim_{n\to\infty} b_n\big)\big]\\ &= \lim_{n\to\infty} d(a_n, b_n).\end{aligned}$$

Hence, we obtain the other inequality and the lemma is proved. □

Theorem 4.3.2 (Completion Theorem for metric spaces)**.** *Let (E,d) be a metric space. Then there exists a complete metric space (E^*,d^*) such that*

(i) (E,d) *is isometric to a subset E_1 of E^*;*

(ii) E_1 *is dense in E^*.*

Moreover, the space (E^*,d^*) is unique up to isometry.

Proof. We will divide the proof into several steps.

Step I (Construction of (E^*,d^*)). In the set of all Cauchy sequences formed by elements of E, we define the following relation,

$$\{a_n\}_{n\in\mathbb{N}} \sim \{b_n\}_{n\in\mathbb{N}} \iff \lim_{n\to\infty} d(a_n,b_n)=0.$$

It easily turns out that $\sim$ is an equivalence relation. Hence, we can define the quotient set

$$E^* = \{[\{a_n\}_{n\in\mathbb{N}}] \mid \{a_n\}_{n\in\mathbb{N}} \text{ is Cauchy}\}.$$

Now we may define a new metric on the set E^*. Let $A=[\{a_n\}_{n\in\mathbb{N}}]$ and $B=[\{b_n\}_{n\in\mathbb{N}}]$ be two elements in E^*. We define

$$d^*(A,B)=\lim_{n\to\infty} d(a_n,b_n).$$

We will show that d^* is a metric defined on E^*. Firstly we have to check that it is well-defined, that is, $d^*(A,B)<+\infty$ and that it does not depend on the representative elements chosen. First we see that $\lim_{n\to\infty} d(a_n,b_n)<+\infty$, i.e., that the sequence of distances $d(a_n,b_n)$ is convergent in $\mathbb{R}$. Since $\mathbb{R}$ is complete, it suffices to check that it is Cauchy. Being Cauchy is clear using the triangle inequality and taking into account that $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are Cauchy:

$$\begin{aligned} d(a_n,b_n)-d(a_m,b_m) &\le d(a_n,a_m)+d(a_m,b_m)+d(b_m,b_n)-d(a_m,b_m)\\ &= d(a_n,a_m)+d(b_m,b_n). \end{aligned}$$

We also have to prove that d^* does not depend on the representative sequences $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$. Assume that

$$A=[(a_n)_{n\in\mathbb{N}}]=[(a'_n)_{n\in\mathbb{N}}] \text{ and } B=[(b_n)_{n\in\mathbb{N}}]=[\{b'_n\}_{n\in\mathbb{N}}].$$

Our aim is to show that $\lim_{n\to\infty} d(a_n,b_n)=\lim_{n\to\infty} d(a'_n,b'_n)$. Using the triangle inequality we get

$$\lim_{n\to\infty} d(a_n,b_n) \le \lim_{n\to\infty}[d(a_n,a'_n)+d(a'_n,b'_n)+d(b'_n,b_n)] = \lim_{n\to\infty} d(a'_n,b'_n).$$

Notice that in the last equality we have $\lim_{n\to\infty} d(a_n,a'_n)=\lim_{n\to\infty} d(b_n,b'_n)=0$ because $(a_n)_{n\in\mathbb{N}}\sim(a'_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}\sim\{b'_n\}_{n\in\mathbb{N}}$. Now, by symmetry we obtain the opposite inequality and hence the desired equality.

It is straightforward to prove that d^* satisfies the axioms of a metric:

M_1) Since $d(a_n, b_n) \geq 0$ it is clear that $d^*(A, B) \geq 0$.

M_2) We have the following chain of equivalences:

$$\begin{aligned} d^*(A,B) = 0 &\iff \lim_{n\to\infty} d(a_n, b_n) = 0 \\ &\iff (a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} \iff A = B. \end{aligned}$$

M_3) It is clear that $d^*(A, B) = d^*(B, A)$ because d also satisfies M_3).

M_4) Let $A = [(a_n)_{n\in\mathbb{N}}]$, $B = [(b_n)_{n\in\mathbb{N}}]$ and $C = [\{c_n\}_{n\in\mathbb{N}}]$ be three elements in E^*. By the triangle inequality of d, for each $n \in \mathbb{N}$ we have $d(a_n, b_n) \leq d(a_n, c_n) + d(c_n, b_n)$. Taking limits, we get $d^*(A, B) \leq d^*(A, C) + d^*(C, B)$.

Thus (E^*, d^*) is a metric space. The following steps are devoted to prove that the new metric space satisfies the required properties.

Step II (E is isometric to a subspace of E^*). Define the map

$$\begin{aligned} \varphi \colon E &\to E^* \\ x &\mapsto \varphi(x) = [\{x\}_{n\in\mathbb{N}}]. \end{aligned}$$

It is well-defined, that is $\varphi(x) \in E^*$, because a constant sequence is always Cauchy. Now we prove that φ is injective:

$$\begin{aligned} \varphi(x) = \varphi(y) &\implies [\{x\}_{n\in\mathbb{N}}] = [\{y\}_{n\in\mathbb{N}}] \implies \{x\}_{n\in\mathbb{N}} \sim \{y\}_{n\in\mathbb{N}} \\ &\implies \lim_{n\to\infty} d(x, y) = 0 \implies d(x, y) = 0 \implies x = y. \end{aligned}$$

Hence, φ restricted to its image is a bijection. Let $E_1 = \varphi(E) \subseteq E^*$. Notice that E_1 is the set of equivalence classes which admit a constant sequence as a representative.

We will prove that $\varphi \colon E \to E_1$ is an isometry. We only have to prove that distances are preserved:

$$d^*(\varphi(x), \varphi(y)) = d^*\left([\{x\}_{n\in\mathbb{N}}], [\{y\}_{n\in\mathbb{N}}]\right) = \lim_{n\to\infty} d(x, y) = d(x, y).$$

Hence $\varphi \colon E \to E_1$ is an isometry and E is isometric to a subset of E^*.

Step III (E_1 is dense in E^*). We have to prove that $E^* = \overline{E_1}$. Of course, it suffices to prove that $E^* \subseteq \overline{E_1}$. Let $A = [(a_n)_{n\in\mathbb{N}}] \in E^*$. We shall see that $A \in \overline{E_1}$ by constructing a sequence of elements in E_1 that converges to A.

For each $k \in \mathbb{N}$ take the constant sequence $\{a_k\}_{n\in\mathbb{N}}$ and the equivalence class $A_k = [\{a_k\}_{n\in\mathbb{N}}] \in E_1$. Our goal is to prove that $\{A_k\}_{k\in\mathbb{N}} \to A$, that is:

$$\forall \varepsilon > 0 \ \ \exists k_0 \in \mathbb{N} \text{ such that } \forall k \geq k_0,\ d^*(A_k, A) = \lim_{n\to\infty} d(a_k, a_n) < \varepsilon.$$

Let $\varepsilon > 0$. Since $(a_n)_{n\in\mathbb{N}}$ is Cauchy, there exists $k_0 \in \mathbb{N}$ such that $d(a_k, a_n) < \varepsilon$ for all $k, n \geq k_0$. Now, taking limits in the last inequality, it follows that

$\{A_k\}_{k\in\mathbb{N}} \to A$, as we wanted to prove.

Step IV (E^* is complete). Let $\{A_n\}_{n\in\mathbb{N}} \subseteq E^*$ be a Cauchy sequence. Our goal is to show that it converges in E^*. Now, for each $k \in \mathbb{N}$, since $A_k \in E^* = \overline{E_1}$, we have that $B\left(A_k, \frac{1}{k}\right) \cap E_1 \neq \varnothing$. Pick $B_k \in B\left(A_k, \frac{1}{k}\right) \cap E_1$. Since $B_k \in E_1$, choose a constant representative element:

$$B_k = [\{b_k\}_{n\in\mathbb{N}}].$$

Now we define a new element,

$$B = [\{b_n\}_{n\in\mathbb{N}}].$$

We will show that our initial sequence $\{A_n\}_{n\in\mathbb{N}}$ converges to B. We have to prove that the element $B \in E^*$ is well-defined, i.e. that the sequence $\{b_n\}_{n\in\mathbb{N}}$ is Cauchy. Using the triangular inequality,

$$\begin{aligned} d(b_p, b_q) = \lim_{n\to\infty} d(b_p, b_q) = d^*(B_p, B_q) &\leq d^*(B_p, A_p) + d^*(A_p, A_q) + d^*(A_q, B_q) \\ &< \frac{1}{p} + \frac{1}{q} + d^*(A_p, A_q). \end{aligned}$$

Now, since the sequence $\{A_n\}_{n\in\mathbb{N}}$ is Cauchy, it is clear that the expression above is arbitrarily small when p and q are big enough; thus the sequence $\{b_n\}_{n\in\mathbb{N}}$ is Cauchy.

Finally, we see that $\{A_n\}_{n\in\mathbb{N}} \to B$. Indeed, we have

$$d^*(A_n, B) \leq d^*(A_n, B_n) + d^*(B_n, B) < \tfrac{1}{n} + \lim_{k\to\infty} d(b_n, b_k).$$

And since $\{b_n\}_{n\in\mathbb{N}}$ is Cauchy, it is clear that $d^*(A_n, B)$ is arbitrarily small for n big enough, that is, $\{A_n\}_{n\in\mathbb{N}} \to B$ and (E^*, d^*) is complete, as we wanted to prove.

Step V (Uniqueness). Assume that (E', d') is another complete metric space satisfying (i) and (ii). By (i), there exists a subset of E', say E_2, such that E_2 is isometric to E. Since being isometric is a equivalence relation, we conclude that E_1 and E_2 are isometric. Call ψ the isometry between E_1 and E_2.

Now we may define an isometry between E^* and E'. To do so, let $A \in E^*$. Since E_1 is dense, there exists a sequence $\{A_k\}_{k\in\mathbb{N}} \subseteq E_1$ such that $\{A_k\}_{k\in\mathbb{N}} \to A$. Now, since $\{A_k\}_{k\in\mathbb{N}}$ is convergent, it is Cauchy, and so the sequence of images $\{\psi(A_k)\}_{k\in\mathbb{N}}$ is also Cauchy in E_2 (because ψ is an isometry).

By completeness, $\{\psi(A_k)\}_{k\in\mathbb{N}}$ is also convergent. Let $A' \in E'$ be its limit. Then let

$$\begin{aligned} \Phi \colon E^* &\to E' \\ A &\mapsto \Phi(A) = A'. \end{aligned}$$

We claim that Φ is an isometry. We have to check that Φ is well-defined, in the sense of A' being independet of the sequence $\{A_k\}_{k\in\mathbb{N}}$. Assume that we have two sequences $\{A_k\}_{k\in\mathbb{N}}$ and $\{\tilde{A}_k\}_{k\in\mathbb{N}}$ converging to A. Let $A' = \lim_{k\to\infty} \psi(A_k)$. Our goal is to see that $A' = \lim_{k\to\infty} \psi(\tilde{A}_k)$, and it follows from the triangle inequality:

$$\begin{aligned}
\lim_{k\to\infty} d'(\psi(\tilde{A}_k), A') &\leq \lim_{k\to\infty} [d'(\psi(\tilde{A}_k), \psi(A_k)) + d'(\psi(A_k), A')] \\
&= \lim_{k\to\infty} d'(\psi(\tilde{A}_k), \psi(A_k)) = \lim_{k\to\infty} d^*(A_k, \tilde{A}_k) \\
&\leq \lim_{k\to\infty} [d^*(A_k, A) + d^*(A, \tilde{A}_k)] = 0.
\end{aligned}$$

To show that Φ is bijective, it suffices if we build an inverse. Of course, in the process of defining Φ we could have started from (E', d') instead of (E^*, d^*), obtaining Φ^{-1}. Hence Φ is bijective.

Using Lemma 4.3.1, it is clear that distances are preserved:

$$\begin{aligned}
d'(\Phi(A), \Phi(B)) = d'(A', B') &= d'\Big(\lim_{k\to\infty} \psi(A_k), \lim_{k\to\infty} \psi(B_k)\Big) \\
&= \lim_{k\to\infty} d'\Big(\psi(A_k), \psi(B_k)\Big) = \lim_{k\to\infty} d^*(A_k, B_k) \\
&= d^*\Big(\lim_{k\to\infty} A_k, \lim_{k\to\infty} B_k\Big) = d^*(A, B).
\end{aligned}$$

This shows that Φ is an isometry and hence the uniqueness is proved. $\square$

Chapter 5

Solved exercises

Problem 1. Given a family of topological spaces $\{(X_i, \tau_i)\}_{i\in I}$ and its product topology $(X = \prod_{i\in I} X_i, \tau_{Tych})$, prove:

(1) The projection $\pi_i\colon (X, \tau_{Tych}) \to (X_i, \tau_i)$ is an open map for each $i \in I$, and it is not necessarily closed.

(2) (X, τ_{Tych}) is T_1 if and only if (X_i, τ_i) is T_1 for each $i \in I$.

(3) (X, τ_{Tych}) is T_2 if and only if (X_i, τ_i) is T_2 for each $i \in I$.

(4) If $A_i \subseteq X_i$ for each $i \in I$, then $\prod_{i\in I} \overline{A_i} = \overline{\prod_{i\in I} A_i}$.

(5) A sequence $(\varphi_n)_{n\in\mathbb{N}}$ is convergent in (X, τ_{Tych}) if and only if the sequence $(\varphi_n(i))_{n\in\mathbb{N}}$ is convergent in (X_i, τ_i) for each $i \in I$.

(6) (X, τ_{Tych}) is totally disconnected if and only if (X_i, τ_i) is totally disconnected for each $i \in I$.

(7) (X, τ_{Tych}) is path-connected if and only if (X_i, τ_i) is path-connected for each $i \in I$.

Solution. (1) We have to prove that for all $U \in \tau_{Tych}$, $\pi_i(U) \in \tau_i$. Since given a map the image of the union is the union of the images and the arbitrary union of open sets is open, it suffices to prove it for basic open sets.
Let $\bigcap_{j\in J} \pi_j^{-1}(U_j) \in \beta_{Tych}$ with $J \subseteq I$ finite. Then

$$\pi_i\Big(\bigcap_{j\in J} \pi_j^{-1}(U_j)\Big) = \begin{cases} U_i \in \tau_i, & \text{if } i \in J, \\ X_i \in \tau_i, & \text{if } i \notin J. \end{cases}$$

Let us see that in general π_i is not closed. Take $(X_1, \tau_1) = (X_2, \tau_2) = (\mathbb{R}, \tau_u)$ so $X = \mathbb{R} \times \mathbb{R}$. Consider the set $C = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy = 1\}$. Moreover, C is closed in X but $\pi_1(C) = \mathbb{R} - \{0\}$ that is not closed in $(\mathbb{R}, \tau_u)$.

(2) Let us suppose that for each $i \in I$, (X_i, τ_i) is T_1. Then given $x \neq y \in X_i$,

there exists $U_i \in \tau_i$ such that $x \in U_i$ and $y \notin U_i$.
Let $\varphi \neq \psi \in X$. Then there exists $i \in I$ such that $\varphi(i) \neq \psi(i)$ and since (X_i, τ_i) is T_1 there exists $U_i \in \tau_i$ such that $\varphi(i) \in U_i$ and $\psi(i) \notin U_i$. Therefore $\varphi \in \pi_i^{-1}(U_i) \in \beta_{Tych} \subseteq \tau_{Tych}$ and $\psi \notin \pi_i^{-1}(U_i) \in \beta_{Tych} \subseteq \tau_{Tych}$, so (X, τ_{Tych}) is T_1.

Now let us prove the other implication. By hypothesis (X, τ_{Tych}) is T_1 so for all $\varphi \neq \psi \in X$, there exists $U \in \tau_{Tych}$ such that $\varphi \in U$ and $\psi \notin U$. Also, there exists $B \in \beta_{Tych}$ such that $\varphi \in B$ and $\psi \notin B$. Given $i \in I$, let us prove that (X_i, τ_i) is T_1 so take $x \neq y \in X_i$. We have to find a set $U_i \in \tau_i$ such that $x \in U_i$ and $y \notin U_i$. Consider $\varphi, \psi \in X$ such that

$$\begin{cases} \varphi(j) = \psi(j) & \text{if } j \neq i \\ \varphi(i) = x \\ \psi(i) = y. \end{cases}$$

Since (X, τ_{Tych}) is T_1 and $\phi \neq \psi$, there exists $B = \bigcap_{j \in J} \pi_j^{-1}(U_j) \in \beta_{Tych}$ such that $\varphi \in B$ and $\psi \notin B$. Then $\varphi(i) = x \in \pi_i(B)$, and for each $k \in J \setminus \{i\}$, $\varphi(k) = \psi(k) \in \pi_k(B)$ so $\psi(i) = y \notin \pi_i(B)$. By (1), π_i is open, so take $U_i = \pi_i(B)$.

(3) This proof is quite similar to the previous one. Let us suppose that for any $i \in I$, (X_i, τ_i) is T_2. Then given $x \neq y \in X_i$, there exist $U_i,\ V_i \in \tau_i,\ U_i \cap V_i = \varnothing$ such that $x \in U_i$ and $y \in V_i$.

Let $\varphi \neq \psi \in X$. Then there exists $i \in I$ such that $\varphi(i) \neq \psi(i)$ and since (X_i, τ_i) is T_2 there exist $U_i,\ V_i \in \tau_i,\ U_i \cap V_i = \varnothing$ such that $\varphi(i) \in U_i$ and $\psi(i) \in V_i$. Therefore $\varphi \in \pi_i^{-1}(U_i) \in \beta_{Tych} \subseteq \tau_{Tych}$ and $\psi \in \pi_i^{-1}(V_i) \in \beta_{Tych} \subseteq \tau_{Tych}$, and $\pi_i^{-1}(U_i) \cap \pi_i^{-1}(V_i) = \pi_i^{-1}(U_i \cap V_i) = \varnothing$ so (X, τ_{Tych}) is T_2.

Now let us prove the other implication. By hypothesis (X, τ_{Tych}) is T_2 so for any $\varphi \neq \psi \in X$, there exist $U,\ V \in \tau_{Tych},\ U \cap V = \varnothing$ such that $\varphi \in U$ and $\psi \in V$. Equivalently, there exist $B_1,\ B_2 \in \beta_{Tych},\ B_1 \cap B_2 = \varnothing$ such that $\varphi \in B_1$ and $\psi \in B_2$. Given $i \in I$, let us prove that (X_i, τ_i) is T_2 so take $x \neq y \in X_i$. We have to find a pair of sets $U_i,\ V_i \in \tau_i,\ U_i \cap V_i = \varnothing$ such that $x \in U_i$ and $y \in V_i$. Consider $\varphi, \psi \in X$ such that

$$\begin{cases} \varphi(j) = \psi(j) & \text{if } j \neq i \\ \varphi(i) = x \\ \psi(i) = y. \end{cases}$$

Since (X, τ_{Tych}) is T_2, there exists $B_1 = \bigcap_{j \in J} \pi_j^{-1}(U_j) \in \beta_{Tych}$ and $B_2 = \bigcap_{j \in J} \pi_j^{-1}(V_j) \in \beta_{Tych},\ B_1 \cap B_2 = \varnothing$ such that $\varphi \in B_1$ and $\psi \in B_2$. Then we have $\psi(i) = y \in \pi_i(B_2)$ and for any $k \in J \setminus \{i\},\ \varphi(k) = \psi(k) \in \pi_k(B_1) \cap \pi_k(B_2)$ so $\varphi(i) = x \in \pi_i(B_1)$. Furthermore, $\pi_i(B_1) \cap \pi_i(B_2) = \varnothing$ because if not, consider $z \in \pi_i(B_1) \cap \pi_i(B_2)$ and then $\sigma \in B_1 \cap B_2$ which is a contradiction, where

$$\sigma(k) = \begin{cases} \varphi(k) = \psi(k) & \text{if } k \in I \smallsetminus \{i\} \\ z & \text{if } k = i. \end{cases}$$

By (1), π_i is open, so take $U_i = \pi_i(B_1)$ and $V_i = \pi_i(B_2)$.

(4) Let us show that $\prod_{i\in I} \overline{A_i} \subseteq \overline{\prod_{i\in I} A_i}$. Consider $\varphi \in \prod_{i\in I} \overline{A_i}$, then for any $i \in I$, $\varphi(i) \in \overline{A_i}$.

Let β_i be basis of τ_i for all $i \in I$. Take a basic neighborhood $C = \bigcap_{j\in J} \pi_j^{-1}(C_j)$ of φ where $C_j \in \beta_j$. Since $\varphi \in C$ it follows that $\varphi(j) \in C_j$, C_j is a basic neighborhood of $\varphi(j)$ and then, for all $j \in J$, by hypothesis $C_j \cap A_j \neq \varnothing$. We can consider the element $\psi \in \prod_{i\in I} X_i$ where

$$\psi(i) = \begin{cases} a_i, & \text{if } i \notin J \\ k_i \in C_i \cap A_i, & \text{if } i \in J, \end{cases}$$

where a_i is in A_i. Then $\psi \in C \cap \prod_{i\in I} A_i$, so $C \cap \prod_{i\in I} A_i \neq \varnothing$. Therefore $\varphi \in \overline{\prod_{i\in I} A_i}$.

Let us prove now the other inclusion. Take $\varphi \in \overline{\prod_{i\in I} A_i}$. By hypothesis for all basic neighborhood B of φ, $B \cap \prod_{i\in I} A_i \neq \varnothing$. Consider the basis of neighborhoods of $\varphi(i)$ consisting of the basic open sets containing the point and take B_i one of them. We have to show that $B_i \cap A_i \neq \varnothing$. Since $\pi_i^{-1}(B_i)$ is a basic open set in X containing φ, it is a basic neighborhood of φ. Then by hypothesis, $\pi_i^{-1}(B_i) \cap \prod_{i\in I} A_i \neq \varnothing$, so there exists $\psi \in \pi_i^{-1}(B_i) \cap \prod_{i\in I} A_i$ and therefore

$$\psi(i) \in \pi_i(\pi_i^{-1}(B_i) \cap \prod_{i\in I} A_i) = B_i \cap A_i.$$

Then $B_i \cap A_i \neq \varnothing$ so $\varphi(i) \in \overline{A_i}$, hence $\varphi \in \prod_{i\in I} \overline{A_i}$.

(5) Suppose $(\varphi_n)_{n\in\mathbb{N}}$ converges to $\varphi \in X$, then since the projections π_i are continuous maps for any $i \in I$ we have that $(\varphi_n(i))_{n\in\mathbb{N}} = (\pi_i(\varphi_n))_{n\in\mathbb{N}}$ converges to $\pi_i(\varphi) = \varphi(i)$.

Now take $(\varphi_n)_{n\in\mathbb{N}}$ and suppose $(\varphi_n(i))_{n\in\mathbb{N}}$ converges to $x_i \in X_i$. Let see that $(\varphi_n)_{n\in\mathbb{N}}$ converges to φ, where $\varphi(i) = x_i$, for each $i \in I$. We have to prove that for all basic neighborhood B of φ there exists $n_0 \in \mathbb{N}$ such that for any $n \geq n_0$, $\varphi_n \in B$. We can consider as basis of neighborhoods of φ the one formed by the basic open sets in X containing the point, so take $B = \bigcap_{j\in J} \pi_j^{-1}(B_j)$ where $B_j \in \beta_j$. Since $\varphi \in B$, then $\varphi(j) \in B_j$, so B_j is a basic neighborhood of $\varphi(j) = x_j$ and by hypothesis there exists $n_j \in \mathbb{N}$ such that for all $n \geq n_j$, $\varphi_n(j) \in B_j$, for each $j \in J$. Since J is finite we can consider $n_0 = \max\{n_j \mid j \in J\}$ and then for any $n \geq n_0$ we have $\varphi_n(j) \in B_j$, for each $j \in J$. Therefore for all $n \geq n_0$, $\varphi_n \in \bigcap_{j\in J} \pi_j^{-1}(B_j) = B$.

(6) To prove this part first we are going to show that

$$C(\varphi) = \prod_{i\in I} C(\varphi(i))$$

$C(\varphi(i))$ is connected for each $i \in I$ and by Theorem 2.1.5 the product of connected sets is connected (with respect to τ_{Tych}) then $\prod_{i\in I} C(\varphi(i))$ is connected. Now $C(\varphi)$ is the largest connected containing φ so $\prod_{i\in I} C(\varphi(i)) \subseteq C(\varphi)$. For the other inclusion, notice that π_i is continuous for each $i \in I$, so $\pi_i(C(\varphi))$ is connected and then $\pi_i(C(\varphi)) \subseteq C(\varphi(i))$, for each $i \in I$. Therefore

$$C(\varphi) = \prod_{i\in I} \pi_i(C(\varphi)) \subseteq \prod_{i\in I} C(\varphi(i)).$$

Now taking this into consideration, we are going to prove the statement easily. Suppose that (X_i, τ_i) is totallly disconnected for each $i \in I$. Then for any $x_i \in X_i$, $C(x_i) = \{x_i\}$. Let $\varphi \in X$, $\varphi(i) \in X_i$ so $C(\varphi(i)) = \{\varphi(i)\}$. Now applying what we have proved,

$$C(\varphi) = \prod_{i\in I} C(\varphi(i)) = \prod_{i\in I} \{\varphi(i)\} = \{\varphi\},$$

so (X, τ_{Tych}) is totally disconnected.
Suppose now that (X, τ_{Tych}) is totally disconnected. Then $\{\varphi\} = C(\varphi) = \prod_{i\in I} C(\varphi(i))$, so $C(\varphi(i)) = \{\varphi(i)\}$. Given $i \in I$, consider (X_i, τ_i) and take $x_i \in X_i$. There exists $\varphi \in X$ such that $\varphi(i) = x_i$. Since (X, τ_{Tych}) is totally disconnected, $C(x_i) = C(\varphi(i)) = \{\varphi(i)\} = \{x_i\}$, so (X_i, τ_i) is totally disconnected.

(7) Suppose (X, τ_{Tych}) is path-connected, and take $x_i, y_i \in X_i$. There exist $\varphi,\ \psi \in X$ such that $\varphi(i) = x_i$ and $\psi(i) = y_i$ and there exists a path $\sigma \colon [0,1] \to X$ such that $\sigma(0) = \varphi$ and $\sigma(1) = \psi$. Since the projections π_i are continuous for each $i \in I$, we can consider $\gamma = \pi_i \circ \sigma \colon [0,1] \to X_i$ which is continuous (being the composition of continuous maps) and $\gamma(0) = \pi_i(\varphi) = \varphi(i) = x_i$ and $\gamma(1) = \pi_i(\psi) = \psi(i) = y_i$, therefore γ is a path between x_i and y_i, so $(X_i \tau_i)$ is path-connected.

Conversely suppose that (X_i, τ_i) is path-connected for each $i \in I$. Take $\varphi,\ \psi \in X$, then for each $i \in I$ there exists a path $\sigma_i \colon [0,1] \to X_i$ such that $\sigma_i(0) = \varphi(i)$ and $\sigma_i(1) = \psi(i)$. Consider now the map $\sigma \colon [0,1] \to X$ such that $\sigma(t) = (\sigma_i(t))_{i\in I}$. Then $\sigma(0) = (\varphi(i))_{i\in I} = \varphi$ and $\sigma(1) = (\psi(i))_{i\in I} = \psi$ and given $\bigcap_{j\in J} \pi_j^{-1}(U_j) \in \beta_{Tych}$,

$$\begin{aligned}
\sigma^{-1}\Big(\bigcap_{j\in J} \pi_j^{-1}(U_j)\Big) &= \{t \in [0,1] \mid (\sigma_i(t))_{i\in I} \in \bigcap_{j\in J} \pi_j^{-1}(U_j)\} \\
&= \{t \in [0,1] \mid \sigma_i(t) \in U_i \text{ for all } i \in J\} = \bigcap_{i\in J} \big(\sigma_i^{-1}(U_i)\big)
\end{aligned}$$

and since σ_i is continuous for each $i \in I$ and J is finite we have that σ is continuous, so σ is a path between φ and ψ, then (X, τ_{Tych}) is path-connected. $\square$

Problem 2. Prove that any subspace of a totally disconnected topological space is totally disconnected.

Solution. If (X, τ) is totally disconnected the unique non-empty connected subsets are the points. For any $A \subseteq X$ take the subspace topology (A, τ_A).

Let $B \subseteq A$ such that $|B| > 1$. We shall see that B is disconnected in (A, τ_A). Since B has got more than two elements it is disconnected in (X, τ). That is, there exists $U, V \in \tau$, such that:

$$\begin{cases} B \subseteq U \cup V \\ B \cap U \cap V = \varnothing \\ B \cap U \neq \varnothing \neq B \cap V. \end{cases}$$

Now, take $U' = U \cap A \in \tau_A$ and $V' = V \cap A \in \tau_A$. Thus,

$$\begin{cases} B = B \cap A \subseteq (U \cup V) \cap A = (U \cap A) \cup (V \cap A) = U' \cup V' \\ B \cap U' \cap V' = B \cap (U \cap A) \cap (V \cap A) = (B \cap A) \cap U \cap V = B \cap U \cap V = \varnothing \\ B \cap U' = B \cap A \cap U = B \cap U \neq \varnothing \neq B \cap V'. \end{cases}$$

Hence, by definition B is disconnected in (A, τ_A); so any subset with more than two elements is disconnected in (A, τ_A). Therefore, the unique connected subsets of (A, τ_A) are the empty set and the points, that is, (A, τ_A) is totally disconnected. $\square$

Problem 3. Prove that every 0-dimensional (every point has a basis of open and closed neighborhoods) and T_1 topological space is totally disconnected.

Solution. Let (X, τ) be the topological space satisfying the conditions in the statement and let $\mathcal{B}_x$ be the basis of open and closed neighborhoods of $x \in X$. X is totally disconnected if for all $x \in X$, $C(x) = \{x\}$, so it suffices to prove that given $A \subseteq X$ with $|A| \geq 2$ then there exist a disconnection of A.

Let $x \neq y \in A$, since X is T_1, there exists $U \in \tau$ such that $x \in U$ and $y \notin U$. Now $U \in \mathcal{N}_x$ implies that there exists $B \in \mathcal{B}_x$ such that $B \subseteq U$, so $x \in B$ and $y \notin B$, implying that $y \in X \setminus B$. Then the following is satisfied:

$$\begin{cases} B,\ X \setminus B \in \tau \\ A \subseteq B \cup (X \setminus B) = X \\ A \cap B \cap (X \setminus B) = \varnothing \\ x \in A \cap B \neq \varnothing \\ y \in A \cap (X \setminus B) \neq \varnothing. \end{cases}$$

Therefore A is disconnected and X is totally disconnected. $\square$

Problem 4. Prove that a compact Hausdorff space (X, τ) is totally disconnected if and only if for each pair $x \neq y$ in X there exists a clopen subset of X containing x but not y.

Solution. The implication from the right to the left is easy: let $x \in X$ and assume by way of contradiction that $|C(x)| \geq 2$. Choose $x \neq y \in C(x)$. Take C_x a clopen subset containing x but not y. Then $C(x) \cap C_x$ is clopen in $C(x)$, it is non-empty (because x is in the intersection) and it is proper (because y is not contained in C_x). Hence $C(x)$ is disconnected, which is a contradiction. Thus, $C(x) = \{x\}$ and X is totally disconnected.

For the converse implication, we define

$$U_x = \bigcap\{C \subseteq X \mid C \text{ clopen and } x \in C\}$$

for each $x \in X$. First we show that $U_x = C(x)$ for all x in X. Once that we have proved that, the conclusion follows, as we will see. Fix $x \in X$..

For the inclusion $C(x) \subseteq U_x$, let $y \in C(x)$ and assume by contradiction that $y \notin U_x$. Then there exists a clopen subset, say C, such that $x \in C$ and $y \notin C$. Now, the subset $C(x) \cap C$ is clopen in $C(x)$, is non-empty (because x is in the intersection) and it is not the whole $C(x)$ because $y \notin C$. Therefore, $C(x)$ is disconnected, a contradiction. So $y \in U_x$, as we wanted..

Now we prove the opposite inclusion. It suffices to show that U_x is connected because $C(x)$ is the biggest connected set containing x. By way of contradiction, suppose that U_x is disconnected, i.e., that there exist $F, G \subseteq U_x$ closed subsets in U_x such that

$$\begin{cases} F \cup G = U_x \\ F \cap G = \varnothing \\ F \neq \varnothing \neq G. \end{cases}$$

Without loss of generality, we shall assume that $x \in F$. U_x is closed (it is the intersection of closed sets) in the compact and Hausdorff space X, hence U_x is compact. Now, $F, G \subseteq U_x$ are closed in the compact and Hausdorff space U_x, and it follows that F and G are compact. We have two compact disjoint sets, F and G, in a T_2 space, and so we know that there exist open sets $U, V \in \tau$ such that

$$\begin{cases} F \subseteq U \\ G \subseteq V, \\ U \cap V = \varnothing. \end{cases}$$

Recall the following property of compactness: if $\{F_i\}_{i \in I}$ is a family of closed sets in X such that the intersection is contained in an open subset, that is, $\cap_{i \in I} F_i \subseteq U \in \tau$, then there exists a finite $J \subseteq I$ such that $\cap_{i \in J} F_i \subseteq U$. Using this property with the compact U_x (notice that $U_x = F \cup G \subseteq U \cup V \in \tau$), there exist $C_1, \ldots, C_k$ clopen subsets such that $x \in C_j$ for all $j \in \{1, \ldots, k\}$ and

$$C := \bigcap_{j=1}^{k} C_j \subseteq U \cup V.$$

Then our new set C is clopen containing x.

Now,

$$\overline{C \cap U} \subseteq \overline{C} \cap \overline{U} = \overline{U} \cap (U \cup V) \cap C = \big(U \cup (\overline{U} \cap V)\big) \cap C \subseteq U \cap C$$

(in the last inclusion we use that $\overline{U} \cap V = \varnothing$. This follows from the fact that $U \subseteq X \smallsetminus V$ so $\overline{U} \subseteq \overline{X \smallsetminus V} = X \smallsetminus V$).

Hence $C \cap U$ is closed (and open, being the intersection of two open sets), so it is clopen. Exchange U and V in the lines above, and we obtain the same for V: the set $C \cap V$ is clopen.

Finally, since $x \in F \subseteq U$ and $x \in C$, we have that $x \in U \cap C$, which we have proved that is a clopen subset. By definition of U_x we have that $U_x \subseteq U \cap C$. Then $\varnothing \neq U_x \cap V \subseteq U \cap C \cap V = \varnothing$, a contradiction. So we have proved that

$$U_x = C(x).$$

Until now, we have not used our assumption of total disconnectedness. Since X is totally disconnected, we have $U_x = \{x\}$ for all $x \in X$.

Let $x \neq y \in X$. Then since

$$x \notin \{y\} = U_y = \bigcap\{C \subseteq X \mid C \text{ clopen and } y \in C\},$$

there exists a clopen subset containing y and not x. Again, since $y \notin \{x\}$, there exists a clopen subset containing x but not y. $\square$

Problem 5. A topological space (X, τ) is said to be *locally compact* if each point in X has a basis of compact neighborhoods. Prove that a locally compact and T_2 space is 0-dimensional if and only if it is totally disconnected.

Solution. Assume that (X, τ) is locally compact, T_2 and totally disconnected. Let $U \in \tau$ and $x \in U$. Since $U \in \mathcal{N}_x$, take $N \in \mathcal{B}_x$, a compact neighborhood of x such that $N \subseteq U$. Then since $N \in \mathcal{N}_x$, there exists an open set, say V, such that $x \in V \subseteq N$, and hence, $\overline{V}$ being a closed subset of a compact Hausdorff space, N, is also a compact neighborhood satisfying $\overline{V} \subseteq U$.

We use the proof of the previous problem with $\overline{V}$ which is compact and Hausdorff, and we obtain that

$$U_x = \bigcap\{C \subseteq X \mid C \text{ clopen in } \overline{V} \text{ and } x \in C\}$$

is equal to $\{x\}$, the connected component of x in $\overline{V}$. Now, since $x \in U_x = \{x\} \subseteq V$ and V is open in $\overline{V}$, by compactness of $\overline{V}$, there exist $C_{1x}, \dots, C_{kx}$ clopen subsets in $\overline{V}$ such that $x \in C_{jx}$ for all $j \in \{1, \dots, k\}$ and $x \in C_{1x} \cap \cdots \cap C_{kx} \subseteq V$. Furthermore, for all $x \in X$, $C_{1x} \cap \cdots \cap C_{kx}$ is clopen in X:

- Firstly, since $C_{1x} \cap \cdots \cap C_{kx}$ is closed in the compact $\overline{V}$, it is compact. Now, X is Hausdorff and $C_{1x} \cap \cdots \cap C_{kx}$ is compact, so it is closed in X.

- On the one hand, $C_{1x} \cap \cdots \cap C_{kx}$ is open in V and on the other hand V is open in X. Hence $C_{1x} \cap \cdots \cap C_{kx}$ is open in X.

Now let $\beta = \{C_{1x} \cap \cdots \cap C_{kx} \mid x \in X\}$. Then β is a basis of (X, τ): we have seen that $\beta \subseteq \tau$. Moreover, by construction of β, given $U \in \tau$ and $x \in U$ there exists $C_{1x} \cap \cdots \cap C_{kx} \in \beta$ such that $x \in C_{1x} \cap \cdots \cap C_{kx} \subseteq V \subseteq U$. This proves that β is a basis (formed by clopen subsets). Then for each $x \in X$, we have that $\mathcal{B}_x = \{B \in \beta \mid x \in B\}$ is a basis of clopen neighborhoods of x, and hence X is 0-dimensional.

The converse implication is already proved in Problem 2 (note that being Hausdorff implies being T_1). $\square$

Problem 6. Prove that the Cantor set (with the usual topology) is homeomorphic to $(\{0,2\}^{\mathbb{N}}, \tau_{Tych})$ and deduce that it is totally disconnected.

Solution. Let $A_0 = [0,1]$, A_1 the set obtained from A_0 deleting its middle third $(1/3, 2/3)$ and in general

$$A_n = A_{n-1} - \bigcup_{k=0}^{3^{n-1}} \left(\tfrac{1+3k}{3^n}, \tfrac{2+3k}{3^n}\right).$$

The Cantor set is defined as the intersection of all them, $C = \bigcap_{n=0}^{\infty} A_n$.[1] Point that A_n is closed for every natural, because so is A_0 and by induction if A_{n-1} is closed A_n is the complement of a union of open sets in A_{n-1}, a closed set, so it is closed in A_{n-1} and therefore in $\mathbb{R}$.

It is evident from the definition that $A_0 \supset A_1 \supset \cdots$. First, we will prove that the elements of the Cantor set are exactly the numbers between 0 and 1 (included) admitting an expansion in base three not containing ones (taking into account that $1 = 0.\overline{2}$ and the same with other positions).

On the one hand, the points we substract in any step are between

$$\left(\frac{1+3k}{3^n}\right)_3 = \left(\frac{k}{3^{n-1}} + \frac{1}{3^n}\right)_3 = 0.\cdots \overbrace{0}^{n\text{th position}} \overline{2}$$

and

$$\left(\frac{2+3k}{3^n}\right)_3 = \left(\frac{k}{3^{n-1}} + \frac{2}{3^n}\right)_3 = 0.\cdots \overbrace{2}^{n\text{th position}} \overline{0},$$

so they must have an expansion in base three of the form

$$0.\cdots \overbrace{1}^{n\text{th position}} \cdots$$

where the 1 in the nth position is not followed by $\overline{2}$ (because that would be the second number written above, which is not substracted), so it does not admit an expression not using the number 1.

On the other hand, suppose that x is a number between 0 and 1 such that its expansion in base three has unavoidable 1's. Suppose that the first unavoidable

[1] See James R. Munkres, *Topology second edition*, Prentice-Hall, 2000, page 176.

1 of the expansion is in nth position. Then if we denote x_{n-1} the previous numbers of the expanxsion we have that the number $0.x_{n-1}\overline{0}$ equals $\frac{k}{3^{n-1}}$ for some $0 \leq k \leq 3^{n-1}$ and therefore

$$x = 0.x_{n-1}1 \cdots \in \Big(\frac{1+3k}{3^n}, \frac{2+3k}{3^n}\Big),$$

which implies that x is not contained in A_n and neither in C.

This allows us to characterize the Cantor set as

$$C = \Big\{\sum_{k=1}^{\infty} \frac{a_k}{3^k} \in [0,1] \mid a_k \in \{0,2\}\Big\}$$

and define a bijection f between this set and the set of sequences of 0's and 2's by

$$f\Big(\sum_{k=1}^{\infty} \frac{a_k}{3^k}\Big) = \{a_k\}_{k\in\mathbb{N}}.$$

Our aim will be proving that f is in fact a homeomorphism between (C, τ_u) and $(\{0,2\}^{\mathbb{N}}, \tau_{Tych})$ (where each factor of the product has the discrete topology). For continuity it suffices to show that

$$U = f^{-1}(\pi_n^{-1}(\{b_n\})) = \Big\{\sum_{k=1}^{\infty} \frac{a_k}{3^k} \in [0,1] \mid a_k \in \{0,2\}, a_n = b_n\Big\}$$

is open in (C, τ_u), where $\{b_n\}$ is the nth factor and b_n belongs to $X = \{0, 2\}$. In fact, the basic open sets of the product topology are *finite* intersections of sets of the form $\pi_n^{-1}(\{b_n\})$ and the preimage of the intersection is the intersection of preimages. We will distinguish two cases, but in both of them the idea will be the same.

Suppose that $b_n = 0$ and consider the set of numbers in C whose decimal expansion is formed by only zeros starting from the nth position,

$$S = \{s \in C \mid s = 0.s_1 \cdots s_{n-1}\overline{0}\} \subset U.$$

Note that S is finite. The idea will be finding for each $s \in S$ the smallest number in $C \setminus U$ greater than s and the greatest number in $C \setminus U$ smaller than s. The case of $s = 0$ is clear, we only have to look for the smallest number in C with a 2 in the nth position in its decimal expansion, and that is clearly $2/3^n$. Now suppose that $s \in S$ is not zero. Again, it is clear that the smallest number of C greater than s and not in U is $s + 2/3^n$. In order to find the greatest number in $C \setminus U$ smaller than s suppose that the last 2 in the expansion of s is in the j_sth position (there must be at least a 2 in the expansion because s is not zero, and $j_s < n$). Then the greatest number in C smaller than s is, with the obvious notation,

$$s' = 0.s_1 \cdots s_{j_s-1}0\overline{2} = s - \frac{1}{3^{j_s}},$$

which is clearly outside U, so is the number we are looking for. We claim that

$$U = C \cap \Big(\bigcup_{s \in S \smallsetminus \{0\}} \Big(s - \frac{1}{3^{j_s}}, s + \frac{2}{3^n} \Big) \cup \Big[0, \frac{2}{3^n} \Big) \Big),$$

which is clearly open in (C, τ_u) (note that C is included in $[0,1]$, so there is no problem taking an interval closed in 0). Indeed, let $x \in U$ and suppose that its first n digits of the expansion are the ones of $s \in S$. Then we have

$$s = 0.s_1 \cdots s_n \overline{0} \leq x = 0.s_1 \cdots s_n \cdots < s + \frac{2}{3^n} = 0.s_1 \cdots s_{n-1} 2 \overline{0}$$

and so $x \in \Big(s - \frac{1}{3^{j_s}}, s + \frac{2}{3^n} \Big)$. Besides, suppose that x does not belong to U and let s be the maximum number in S smaller than x (the one whose first $n-1$ digits coincide). Then

$$s + \frac{2}{3^n} = 0.x_1 \cdots x_n \overline{0} \leq x$$

and so $x \notin \Big(s - \frac{1}{3^{j_s}}, s + \frac{2}{3^n} \Big)$. Now, let s' be the minimum number in S greater than x (if such number exists) and suppose that the first $j \geq 0$ digits of the decimal expansion of x and s' coincide. Since $s' > x$ we have that the jth digit of s' must be 2 and the one of x must be 0, so $j_{s'} \geq j$ and

$$s' - \frac{1}{3^{j_{s'}}} \geq 0.s_{j-1} 0 \overline{2} \geq x$$

and so $x \notin \Big(s - \frac{1}{3^{j_{s'}}}, s + \frac{2}{3^n} \Big)$. Finally, point that if $s, s' \in S$ and $s < s'$ we have that there exists $j < n$ such that the jth number in the expansion of s is a 0 and a 2 in the one of s' (with $s_{j-1} = s'_{j-1}$). Thus,

$$s + \frac{2}{3^n} < 0.s_1 \cdots s_{j-1} 0 \overline{2} \leq 0.s'_1 \cdots s'_{j_{s'}-1} 0 \overline{2} = s' - \frac{1}{3^{j_{s'}}},$$

so the intervals we have used to construct U are disjoint.

When $b_n = 1$ the idea is exactly the same, but the construction of the intervals is slightly different. Consider the set of numbers in C whose decimal expansion is formed by only 2's starting from the nth position and has a two in the nth position,

$$S = \{ s \in C \mid s = 0.s_1 \cdots s_{n-1} \overline{2} \} \subset U.$$

For $s = 1 = 0.\overline{2}$ we must find a number in $C \smallsetminus U$, which is clearly $1 - 2/3^n$. Now, let $1 \neq s \in S$. The greatest number in $C \smallsetminus U$ smaller than s is clearly $s - 2/3^n$. For the smallest number in $C \smallsetminus U$ greater than s suppose that the last zero in the expansion of s is in the j_sth position (there is at least a zero since s is not 1). Then the smallest number in C greater than s is, taking into account that the zero must be followed by 2's,

$$s' = 0.s_1 \cdots s_{j_s - 1} 2 \overline{0} = s + \frac{1}{3^{j_s}},$$

which is clearly outside U. We claim that

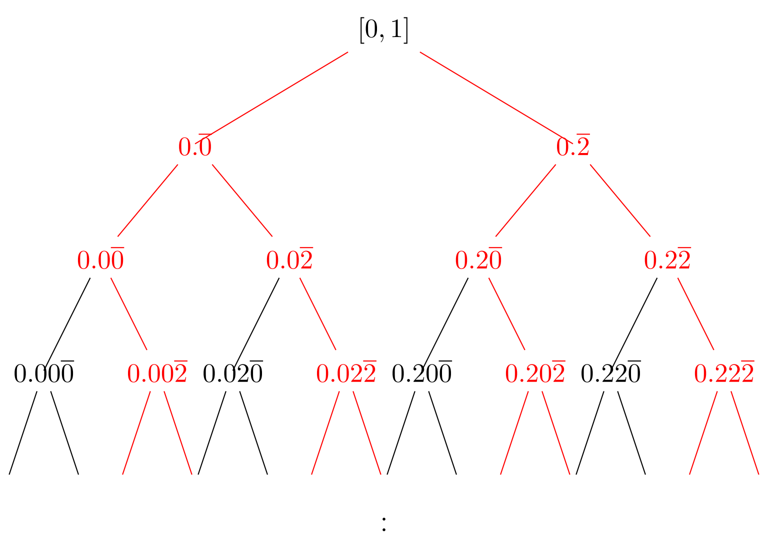
$$U = C \cap \Big(\bigcup_{s \in S \setminus \{1\}} \Big(s - \frac{2}{3^n}, s + \frac{1}{3^{j_s}} \Big) \cup \Big(1 - \frac{2}{3^n}, 1 \Big] \Big),$$

which is, with the same argument, open in (C, τ_u). Indeed, let $x \in U$ and suppose that its first n digits of the expansion are the ones of $s \in S$. Then we have

$$s = 0.s_1 \cdots s_n \overline{2} \geq x = 0.s_1 \cdots s_n \cdots > s - \frac{2}{3^n} = 0.s_1 \cdots s_{n-1} 0 \overline{2}$$

and so $x \in \Big(s - \frac{2}{3^n}, s + \frac{1}{3^{j_s}} \Big)$. The process to show that if x is not in U then it is not in the intervals we have constructed is also very similar, so we won't reproduce everything again.

There is a visual way of representing all this, using a tree and concieving the different paths as the numbers of C. The vertices are now the endpoints of the intervals we obtain in each "level" A_n base three (which are also paths), and the open set we have been determining before is formed by the paths that reach an odd vertex ($b_n = 0$) or an even vertex ($b_n = 2$) in the nth level . For example, in the following tree the paths (numbers) contained in $f^{-1}(\pi_2^{-1}(\{2\}))$ are marked in red:



As the reader can perceive, the way of obtaining the numbers of higher levels is quite systematic ($\overline{0}$ to the left, $\overline{2}$ to the right), and in fact can be very helpful to visualize the smallest point in C greater than a vertex (the number it represents) or the greatest point in C smaller than it. Of course, pictures are not formal proofs, so the prolix work done before was necessary.

Until the moment we have shown bijectivity and continuity, but that is not enough to ensure that f is a homeomorphism. However, it is relatively easy to show that our map is closed. On the one hand, by part (3) of Problem 1 we know that $(\{0,2\}^{\mathbb{N}}, \tau_{Tych})$ is T_2, because so is $(\{0,2\}, \tau_{dis})$. On the other hand, the Cantor set is clearly bounded and closed, so it is compact. Therefore, we have a continuous map from a compact space to a Hausdorff space, so it is closed.

Finally, $(\{0,2\}, \tau_{dis})$ is totally disconnected because it is discrete, so the topological space $(\{0,2\}^{\mathbb{N}}, \tau_{Tych})$ is also totally disconnected according to part (4) of Problem 1. Hence, since connection is a topological property, so are disconnection and total disconnection and C must be totally disconnected. $\square$

Problem 7. Let A be a countable subset of $\mathbb{R}^2$. Prove that $\mathbb{R}^2 \smallsetminus A$ is path-connected in $\mathbb{R}^2$.

Solution. Let $x \neq y$ in $\mathbb{R}^2 \smallsetminus A$. Let $L_{xy} \subseteq \mathbb{R}^2$ be the line joining x and y. Let N_{xy} be the perpendicular bisector of the segment between x and y. For each $z \in N_{xy}$, denote by $R_{xzy} = L_{xz} \cup L_{zy}$, the union of the lines joining x and z, and z and y. We have that $R_{xzy} \cap R_{xz'y} = \{x, y\}$ whenever $z \neq z'$ in N_{xy} and, since there are uncountably many R_{xzy} and A is countable, we have that there exists $z_0 \in N_{xy}$ such that $R_{xz_0y} \cap A = \varnothing$ i.e. $R_{xz_0y} \subseteq \mathbb{R}^2 \smallsetminus A$. Then we have a continuous path joining x and y and consisting of two line segments and thus $\mathbb{R}^2 \smallsetminus A$ is path-connected. $\square$

Problem 8. Prove that if U is open and connected in $(\mathbb{R}^n, \tau_u)$, then it is path-connected.

Solution. According to Proposition 2.5.12 it suffices to show that under these conditions U is locally path-connected. But it follows easily from the fact that U is open, because that allows us to construct a local base of balls for its points. Indeed, let $x \in U$. Since U is open, there exists $\varepsilon_x > 0$ such that $B(x, \varepsilon_x) \subset U$, so we can choose as local base

$$\mathcal{B}_x = \{B(x, \varepsilon) \subset U \mid 0 < \varepsilon < \varepsilon_x\}.$$

Since balls in $\mathbb{R}^n$ are path-connected (in fact they are convex sets) we conclude that U is locally path-connected, as desired. $\square$

Problem 9. Prove that any quotient of a locally connected topological space is locally connected.

Solution. According to Theorem 2.5.11 it is enough to see that the connected components of any open subset in the quotient space are open.

Let X be a locally connected space, $\sim$ an equivalence relation on X and $p\colon (X, \tau_X) \to (X/\!\sim, \tau_{quot})$ the natural projection. Let A be an open subset of $X/\!\sim$ and C the connected component of $p(x)$ for a representative $x \in p^{-1}(A) \in \tau$. We shall prove that $p^{-1}(C)$ is the union of some connected components of $p^{-1}(A)$, which according to the above theorem are open. Let K_y be the connected component of any y in $p^{-1}(A)$. As p is continuous $p(K_y) \subseteq A$ is connected and contains $p(y)$, hence by the definition of C, $p(K_y) \subseteq C$, so $K_y \subseteq p^{-1}(C)$. Thus,

$$\bigcup_{y \in p^{-1}(C)} K_y \subseteq p^{-1}(C)$$

and the inverse inclusion is clear.

Since $p^{-1}(C)$ is the union of some open subsets it is open in X, i.e., C is open in $X/\sim$. Thus, according to Theorem 2.5.11 $(X/\sim, \tau_{quot})$ is locally connected. □

Problem 10. Prove that a topological space is totally disconnected and locally connected if and only if it is discrete.

Solution. ⇒) If (X, τ) is totally disconnected the unique non-empty connected elements are the singletons.

Futhermore (X, τ) is locally connected, let $\mathcal{B}_x$ be a neighborhood basis of each x in X with connected elements. Since it is a neighborhood basis of x, for all $x \in X$ exists $B_x \in \mathcal{B}_x$ such that $x \in B_x$ and B_x is connected, i.e., $B_x = \{x\}$. Thus, $\{x\}$ is a neighborhood of x, and by definition exists an open set $U_x \in \tau$ such that $x \in U_x \subseteq \{x\}$. Therefore, $U_x = \{x\}$, so all the singletons are open. That is, τ is the discrete topology as we were required.

⇐) If $(X, \tau) = (X, \tau_{dis})$ the set A is connected if and only if $|A| \leq 1$.

Thus, for any $x \in X$ its connected component in X is $\{x\}$. Since, the point is a connected set that contains x, and it is impossible to get a connected set containing more than one element. Hence, (X, τ_{dis}) is totally disconnected.

Futhermore, in the discrete topology, $C(x) = \{x\}$ is open for all $x \in X$. Then $C(x)$ is a connected neighborhood for each $x \in X$, and $\mathcal{B}_x = \{\{x\} \mid x \in X\}$ is a connected neighborhood basis of X. Hence, (X, τ) is locally connected. □

Problem 11. Given a family of topological spaces $\{(X_i, \tau_i)\}_{i \in I}$ and its product topology $(X = \prod_{i \in I} X_i, \tau_{Tych})$, prove that (X, τ_{Tych}) is locally connected if and only if (X_i, τ_i) is locally connected for all $i \in I$ and (X_i, τ_i) is connected except, at most, for finitely many of them.

Solution. ⇒) Assume that (X, τ_{Tych}) is locally connected. First we show that (X_i, τ_i) is locally connected for all $i \in I$, i.e., that is has a basis of connected neighbourhoods for each point. Let $i \in I$ and $x_i \in X_i$. Choose $\varphi \in X$ such that $\varphi(i) = x_i$. Let $\mathcal{B}_\varphi$ be a basis of connected neighbourhoods of φ (here we are using that X is locally connected). We first easily will see that

$$\pi_i(\mathcal{B}_\varphi) = \{\pi_i(B_\varphi) \mid B_\varphi \in \mathcal{B}_\varphi\}$$

is a basis of neighbourhoods of $x_i \in X_i$:

- For all $B_\varphi \in \mathcal{B}_\varphi$, there exists $U_\varphi \in \tau_{Tych}$ such that $\varphi \in U_\varphi \subseteq B_\varphi$ and so $x_i \in \pi_i(U_\varphi) \subseteq \pi_i(B_\varphi)$ with $\pi_i(U_\varphi)$ open in X_i (because the map π_i is open). Hence $\pi_i(\mathcal{B}_\varphi) \subseteq \mathcal{N}_{x_i}$.

- Let $N \in \mathcal{N}_{x_i}$. Then there exists $U \in \tau_i$ such that $x_i \in U \subseteq N$. Hence $\varphi \in \pi_i^{-1}(U) \subseteq \pi_i^{-1}(N)$, with $\pi_i^{-1}(U)$ open in the product because π_i is continuous; and so, $\pi_i^{-1}(N) \in \mathcal{N}_\varphi$. Since $\mathcal{B}_\varphi$ is a basis of neighborhoods of φ, there exists $B_\varphi \in \mathcal{B}_\varphi$ such that $B_\varphi \subseteq \pi_i^{-1}(N)$. Thus, $\pi_i(B_\varphi) \subseteq \pi_i(\pi_i^{-1}(N)) = N$ (in the last equality we use that π_i is surjective).

Hence $\pi_i(\mathcal{B}_\varphi)$ is a basis of neighborhoods of x_i. Furthermore, since all $B_\varphi \in \mathcal{B}_\varphi$ are connected and π_i is continuous, it follows that $\pi_i(\mathcal{B}_\varphi)$ is a basis of connected neighbourhoods. This proves that (X_i, τ_i) is locally connected.

Moreover, we have to show that (X_i, τ_i) are connected perhaps except finitely many of them. We fix $\varphi_0 \in X$ and let B be a connected neighbourhood of φ_0 (here we're using the local connectedness again). Since B is a neighbourhood, there exists $\cap_{j\in J}\pi_j^{-1}(U_j) \in \beta_{Tych}$ (with $J \subseteq I$ finite and $U_j \in \tau_j$ for all $j \in J$) satisfying $\bigcap_{j\in J} \pi_j^{-1}(U_j) \subseteq B$. Moreover, we have that

$$\bigcap_{j\in J} \pi_j^{-1}(U_j) = \bigcap_{j\in J} \prod_{i\in I} V_{i,j} \quad \text{and} \quad V_{i,j} = \begin{cases} X_i & \text{if } i \neq j \\ U_j & \text{if } i = j. \end{cases}$$

Then for all $i \notin J$,

$$\pi_i\Big(\bigcap_{j\in J} \pi_j^{-1}(U_j)\Big) = X_i \subseteq \pi_i(B),$$

so we get the equality $X_i = \pi_i(B)$. Since π_i is continuous and B is connected, we have that $\pi_i(B) = X_i$ is connected for all $i \notin J$, that is, X_i is connected except for finitely many values of $i \in I$.

$\Leftarrow$) Let $\varphi \in X$ and $N \in \mathcal{N}_\varphi$. Then there exists $\cap_{j\in J}\pi_j^{-1}(U_j) \in \beta_{Tych}$ (with $J \subseteq I$ finite and $U_j \in \tau_j$ for all $j \in J$) such that $\varphi \in \bigcap_{j\in J} \pi_j^{-1}(U_j) \subseteq N$. Then we have

$$\bigcap_{j\in J} \pi_j^{-1}(U_j) = \bigcap_{j\in J} \prod_{i\in I} V_{i,j} \quad \text{and} \quad V_{i,j} = \begin{cases} X_i & \text{if } i \neq j \\ U_j & \text{if } i = j. \end{cases}$$

We shall assume that X_i is connected for all $i \notin J$: in fact, since there are finitely many disconnected X_i, we could insert the indexes $i \notin J$ for which X_i isn't connected in the set J and take $U_j = X_j$ for those indexes. Of course, the basic open does not change but now for all $i \notin J$, we have that X_i is connected.

Let $J' = J \cup \{i \in I \mid X_i \text{ is disconnected}\}$ and take $U_i = X_i$ for each $i \in J' \setminus J$. Now, for each $i \in J'$, we have $\varphi(i) \in U_i \in \tau_i$, so $U_i \in \mathcal{N}_{\varphi(i)}$. Thus, since (X_i, τ_i) is locally connected, there exists some connected basic neighborhood B_i of $\varphi(i)$ with $B_i \subseteq U_i$. Then define

$$B_N = \prod_{i\in I} V_i \quad \text{with} \quad V_i = \begin{cases} B_i & \text{if } i \in J' \\ X_i & \text{otherwise.} \end{cases}$$

By Theorem 2.1.5, B_N is connected in the product. It is also clear (taking into account that $B_i \subseteq U_i$ for each $i \in J'$) that

$$\varphi \in \bigcap_{i\in J'} \pi_i^{-1}(U_i) \subseteq B_N.$$

Hence, B_N is a connected neighborhood of φ satisfying $B \subseteq N$. This proves that if we set $\mathcal{B}_\varphi = \{B_N \mid N \in \mathcal{N}_\varphi\}$, it is a basis of connected neighborhoods of φ and so X is locally connected. $\square$

Part II

Algebra

Chapter 6

p-adic numbers

6.1 Foundations

6.1.1 Absolute values on fields

Definition 6.1.1. Let K be a field. An *absolute value* on K is a function

$$| \ |: K \to \mathbb{R}$$

satisfying

(i) $|x| = 0$ if and only if $x = 0$.

(ii) $|xy| = |x||y|$ for all $x, y \in K$.

(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

We will say that an absolute value is *non-archimedean* if it satisfies the additional condition

(iv) $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$.

Otherwise, we will say that the absolute value is *archimedean*.

Note that condition (iv) above implies condition (iii).

Example 6.1.2. Let K be a field. Then

$$|x| = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

is an absolute value, which is said to be the *trivial absolute value*.

Definition 6.1.3. Let K be a field. A map $\nu: K \to \mathbb{R} \cup \{+\infty\}$ is said to be a *valuation* if it satisfies the following conditions:

(i) $\nu(x) = +\infty$ if and only if $x = 0$.

(ii) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in K$.

(iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in K$.

In case that $\nu\colon K \to \mathbb{Z} \cup \{+\infty\}$, we shall say that ν is a *discrete valuation.*

If we are given a valuation ν, we can fix any $c > 1$ and define $|x| = c^{-\nu(x)}$ which turns out be an absolute value (here we understand that $c^{-\infty} = 0$). Indeed, the minus sign reverses the inequality and the exponential turns the sum into a product. Furthermore, this absolute value obtained from the valuation is a non-archimedean absolute value.

Now, we introduce one of the main examples of the chapter.

Example 6.1.4 (p-adic valuation and absolute value on $\mathbb{Q}$)**.** Let p be a prime number. Given $\frac{a}{b} \in \mathbb{Q} \setminus \{0\}$, let n be the only integer such that

$$\frac{a}{b} = p^n \frac{a'}{b'}$$

with $p \nmid ab$ (that is, $p \nmid a$ and $p \nmid b$). Define

$$\nu_p\left(\frac{a}{b}\right) = \begin{cases} n & \text{if } \frac{a}{b} \neq 0 \\ +\infty & \text{otherwise.} \end{cases}$$

Then ν_p is a valuation, called the *p-adic valuation.* Moreover, the non-archimedean absolute value

$$|x|_p = p^{-\nu(x)}$$

is called the *p-adic absolute value.*

In particular, $|p|_p = \frac{1}{p}$ and $|p^n|_p = \frac{1}{p^n}$, for all $n \in \mathbb{Z}$. To get an intuition of what the p-adic absolute value does, it measures how divisible by p a number is.

We can generalize the previous example to the case of an arbitrary unique factorization domain:

Example 6.1.5. (1) Let A be a unique factorization domain (UFD) and K its field of quotients. Let $p \in A$ be an irreducible element. Then we can define the p-adic valuation on K. Indeed, take $a \in A \setminus \{0\}$, and let n be the unique (and here is where we use the unique factorization) non-negative integer such that

$$a = p^n a' \quad \text{and} \quad p \nmid a'$$

and let $\nu_p(a) = n$. Then

$$\nu_p\left(\frac{a}{b}\right) = \begin{cases} \nu_p(a) - \nu_p(b) & \text{if } \frac{a}{b} \neq 0 \\ +\infty & \text{otherwise} \end{cases}$$

is a valuation defined on K, called the *p-adic valuation*. We have to show that the expression above does not depend on the representation as a fraction: take $\frac{a}{b} = \frac{c}{d} \in K$. If $\frac{a}{b} = \frac{c}{d} = 0$, it is clear that $\nu_p\left(\frac{a}{b}\right) = \nu_p\left(\frac{c}{d}\right) = +\infty$. Hence, assume that $a, b, c, d \neq 0$. Then since $ad = cb$, we have

$$\begin{aligned}\nu_p(ad) = \nu_p(cb) &\implies \nu_p(a) + \nu_p(d) = \nu_p(c) + \nu_p(b) \\ &\implies \nu_p(a) - \nu_p(b) = \nu_p(c) - \nu_p(d) \implies \nu_p\left(\frac{a}{b}\right) = \nu_p\left(\frac{c}{d}\right)\end{aligned}$$

and so the valuation is well-defined.

(2) The p-adic valuation of $\mathbb{Q}$ defined in Example 6.1.4 is a particular case of the previous item (1), when $A = \mathbb{Z}$.

(3) Let F be a field. Then $F[t]$ is a unique factorization domain and so we can define the $p(t)$-adic valuation on the field of quotients $F(t)$, for any irreducible polynomial $p(t) \in F[t]$.

(4) Let F be a field. Define

$$\nu\left(\frac{f(t)}{g(t)}\right) = \deg g - \deg f$$

for all $f, g \in F[t]$. Then ν is a valuation defined on the field $F(t)$. However, this is not a new type of valuation because in Problem 14 we show that it is actually a $\frac{1}{t}$-adic valuation, constructed starting from the UFD $F\left[\frac{1}{t}\right]$, whose field of quotients is $F(t)$.

6.1.2 Basic properties

The following lemma shows some basic properties of the absolute values.

Lemma 6.1.6. *For any absolute value $|\ |$ on any field K, we have:*

(i) $|1| = 1$.

(ii) *If $x \in K$ and $|x^n| = 1$, then $|x| = 1$.*

(iii) $|-1| = 1$.

(iv) *If K is a finite field, then $|\ |$ is trivial.*

Proof. (i) We have $|1| = |1^2| = |1||1| = |1|^2$ and since $|1|$ is a non-negative real number, $|1| = 1$.

(ii) $|x|^n = |x^n| = 1$ and then $|x|$ is a non-negative real nth root of unity, hence $|x| = 1$.

(iii) $|(-1)^2| = |1| = 1$ and by (ii), it follows that $|-1| = 1$.

(iv) We prove this part in Problem 12.

∎

The following theorem gives us a method to decide whether one absolute value is archimedean or not.

Theorem 6.1.7. *Let K be a field and $A = \{n1_K \mid n \in \mathbb{Z}\} \subseteq K$ the image of $\mathbb{Z}$ in K. An absolute value $|\ |$ on K is non-archimedean if and only if $|a| \leq 1$ for all $a \in A$. In particular, an absolute value on $\mathbb{Q}$ is non-archimedean if and only if $|n| \leq 1$ for every $n \in \mathbb{Z}$.*

Proof. One part is easy: write $a = n1_K$. If $n > 0$,

$$|a| = |n1_K| = |1_K + \overset{n}{\cdots} + 1_K| \leq \max\{|1_K|, \overset{n}{\cdots}, |1_K|\} = 1.$$

Similarly, if $n < 0$,

$$|a| = |n1_K| = |-1_K - \overset{n}{\cdots} - 1_K| \leq \max\{|-1_K|, \overset{n}{\cdots}, |-1_K|\} = 1$$

and by definition $|0| = 0 \leq 1$.

Let us prove the converse. Let $x, y \in K$. Our aim is to show that

$$|x + y| \leq \max\{|x|, |y|\}.$$

If $y = 0$, it is trivial, so let us assume $y \neq 0$. It is equivalent to prove:

$$\left|\frac{x}{y} + 1\right| \leq \max\left\{\left|\frac{x}{y}\right|, 1\right\}$$

(just multiply by the non-negative number $|y|$). In other words, we want to prove that

$$|x + 1| \leq \max\{|x|, 1\}$$

for all $x \in K$. Now let m be any positive integer. Then

$$|x+1|^m = |(1+x)^m| = \left|\sum_{k=0}^{m}\binom{m}{k}x^k\right| = \left|\sum_{k=0}^{m}\left(\binom{m}{k}1_K\right)x^k\right|$$
$$\leq \sum_{k=0}^{m}\left|\binom{m}{k}1_K\right|\left|x^k\right|.$$

By hypothesis, we have that $\left|\binom{m}{k}1_K\right| \leq 1$ for all $k \in \{0 \ldots, m\}$. Then we obtain that

$$|x+1|^m \leq \sum_{k=0}^{m}\left|x^k\right|.$$

Now we distinguish two cases. On the one hand, if $|x| > 1$, we have that $|x|^k \leq |x|^m$ for all $k \in \{0, 1, \ldots, m\}$. On the other hand, if $|x| \leq 1$, clearly $|x|^k \leq 1$ for all $k \in \{0, 1, \ldots, m\}$. Hence, in any case, $|x|^k \leq \max\{|x|^m, 1\}$ for all $k \in \{0, 1, \ldots, m\}$. Finally we conclude that

$$|1 + x|^m \leq (m+1)\max\{|x|^m, 1\}.$$

Extracting mth roots, we get

$$|x+1| \leq \sqrt[m]{m+1}\max\{|x|, 1\}.$$

Finally, taking limits when $m \to \infty$,

$$|x+1| \leq \max\{|x|, 1\}$$

as we wanted to prove. $\square$

It is known that the real numbers satisfy the archimedean property, that is, given two real numbers $x, y \in \mathbb{R}$, $x > 0$, there exists $n \in \mathbb{N}$ such that $nx > y$, or equivalently, if $x \neq 0$, $|nx| > |y|$. Now, if we are given an archimedean absolute value, we will see that the archimedean property holds. Indeed, if $|\ |$ is archimedean, by Theorem 6.1.7, there exists $a \in A$ such that $|a| > 1$, and hence $\lim_{n\to\infty} |a|^n = +\infty$, implying that

$$\sup\{|a| : a \in A\} = +\infty.$$

Let $x, y \in K$ with $x \neq 0$. Then there exists $a = n1_K \in A$, such that $|n1_k| > |\frac{y}{x}|$, or, equivalently, $|nx| > |y|$, that is, the archimedean property holds.

Similarly, we get the following corollary for non-archimedean absolute values:

Corollary 6.1.8. *An absolute value $|\ |$ is non-archimedean if and only if*

$$\sup\{|n1_K| \colon n \in \mathbb{Z}\} = 1.$$

6.1.3 Topology

Definition 6.1.9. Let K be a field and $|\ |$ an absolute value on K. We define the *distance* $d(x, y)$ between two elements $x, y \in K$ by

$$d(x, y) = |x - y|.$$

The function $d(x, y)$ is a metric and it is called the *metric induced by the absolute value.*

We know that the inequality $|x + y| \leq |x| + |y|$ implies $d(x, y) \leq d(x, z) + d(z, y)$, the *triangle inequality.* Furthermore, if $|\ |$ is non-archimedean, we have the following lemma:

Lemma 6.1.10. *Let $|\ |$ be an absolute value on a field K and define a metric by $d(x, y) = |x - y|$. Then $|\ |$ is non-archimedean if and only if for all $x, y, z \in K$ we have*

$$d(x, y) \leq \max\{d(x, z), d(z, y)\}.$$

Proof. To go one way, apply the non-archimedean property to the equation

$$(x - y) = (x - z) + (z - y).$$

For the converse, let $x', y' \in K$ and choose $x = x'$, $y = -y'$, $z = 0$, to obtain $d(x', -y') \leq \max\{d(x', 0), d(0, -y')\}$, that is,

$$|x' + y'| \leq \max\{|x'|, |y'|\}.$$

□

Definition 6.1.11. The inequality

$$d(x, y) \leq \max\{d(x, z), d(z, y)\}$$

is called the *ultrametric inequality*, and in that case the metric d is called *ultrametric*. A space equipped with an ultrametric is called an *ultrametric space*.

Now we will give some properties of ultrametric spaces.

Proposition 6.1.12. *In an ultrametric space, all triangles are isosceles with the two longest sides equal.*

Proof. Assume that x, y and z are the vertices of the triangle. Then the lengths of the sides are $d(x, y), d(x, z)$ and $d(y, z)$. Without loss of generality assume that $d(x, y)$ is the longest one. Now, assume by way of contradiction that the other sides are less than $d(x, y)$, that is, $d(x, z) < d(x, y)$ and $d(z, y) < d(x, y)$. But then $d(x, y) > \max\{d(x, z), d(z, y)\}$, contradicting the ultrametric inequality. □

Let (X, d) be a metric space. Recall that the set

$$B(a, r) = \{x \in X \mid d(x, a) < r\}$$

is called the *open ball* of center a and radius r; and the set

$$\overline{B}(a, r) = \{x \in X \mid d(x, a) \leq r\}$$

is called the *closed ball* of center a and radius r. Open balls are open sets and closed balls are closed sets in the topology defined by any metric d.

For ultrametric spaces, we get some surprising properties:

Proposition 6.1.13. *Let (X, d) be an ultrametric space. Then*

(i) *Any point of an open (closed) ball is the center of the ball.*

(ii) *Any two open (closed) balls are either disjoint or the one with smallest radius is contained in the other.*

(iii) *All open balls are closed and all closed balls of radius $r > 0$ are open.*

Proof. (i) Let $r \geq 0$ and $x \in K$. We have to see that for all $y \in B(x, r)$, $B(x, r) = B(y, r)$. By symmetry (we can exchange x and y), it suffices to prove only one inclusion. Let $z \in B(y, r)$, then

$$d(x, z) \leq \max\{d(x, y), d(y, z)\} < r$$

and so $z \in B(x, r)$. To prove the case of closed balls, we only need to replace $<$ with $\leq$ in the proof above.

(ii) Assume first that $B(x,r) \cap B(y,s) \neq \varnothing$. Let $z \in B(x,r) \cap B(y,s)$. Since $z \in B(y,s)$, by part (i) it follows that $B(z,s) = B(y,s)$. Similarly, using part (i), we have $B(z,r) = B(x,r)$. Then $B(x,r) \subseteq B(y,s)$ or $B(y,s) \subseteq B(x,r)$, according to $r \leq s$ or $s \leq r$. The case of the closed balls is identical.

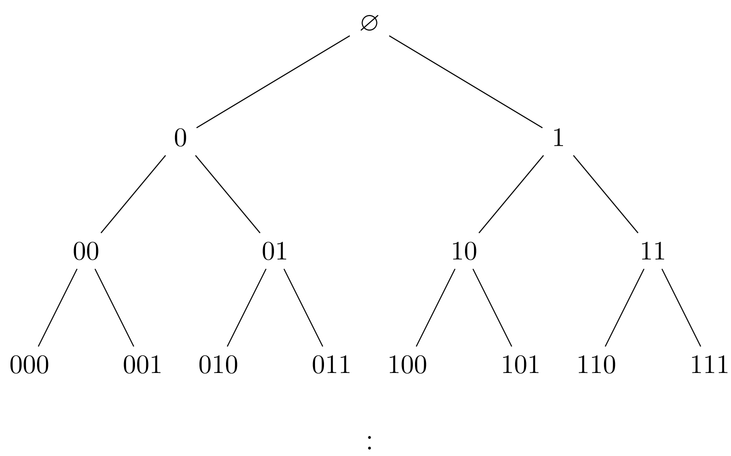
(iii) First we prove that open balls are closed. Let $y \in \overline{B(x,r)}$, that is, for all $s > 0$, $B(x,r) \cap B(y,s) \neq \varnothing$. By the proof of (ii), if we take $s < r$, then $B(y,s) \subseteq B(x,r)$ and hence $y \in B(x,r)$.

Now we prove that closed balls are open. Let $r > 0$ and $y \in \overline{B}(x,r)$. Then using item (i), we have that $\overline{B}(y,r) = \overline{B}(x,r)$. Now, choose s such that $0 < s < r$. Then we have that $y \in B(y,s) \subseteq \overline{B}(y,s) \subseteq \overline{B}(y,r) = \overline{B}(x,r)$ and hence $y \in \operatorname{int}(\overline{B}(x,r))$, and $\overline{B}(x,r)$ is open.

□

The following example gives us an intuitive idea of how ultrametric balls are:

Example 6.1.14. Let X be a finite set (we will say that X is the *alphabet*) and denote by X^* the set words in X, which is called the *free monoid* on X. Let us examine the case $X = \{0,1\}$. We can represent all the words in an infinite tree:



Notice that we have infinitely many infinite paths in the tree. These paths are infinite words, or, equivalently, each path can be thought as a sequence. Let X^ω be the set of all the infinite paths in the tree.

Now, we want to define a distance in X^ω. Assume $p, q \in X^\omega$ are two paths (that is, two infinite words) which coincide exactly at the first r symbols. Then

$$d(p,q) = 2^{-r}$$

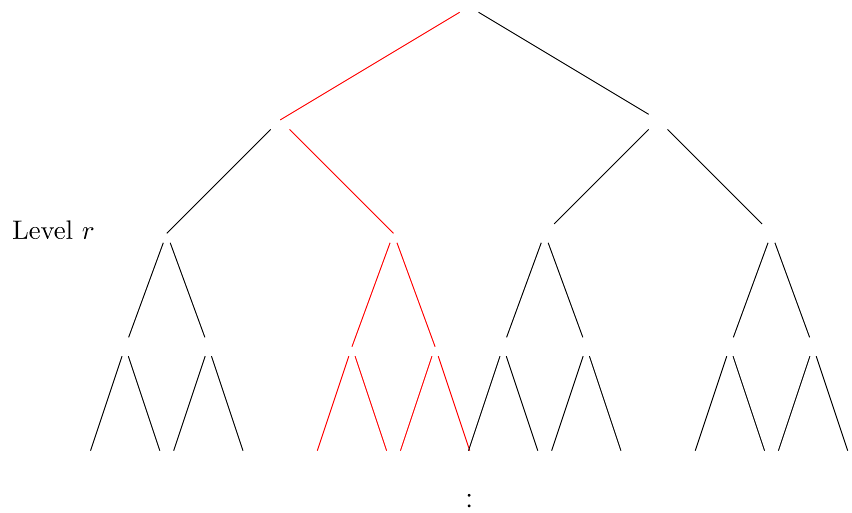
is an ultrametric and (X^ω, d) is a ultrametric space. Actually, we can define d in a more general way. Let $\{a_n\}_{n \in \mathbb{N}}$ be a strictly decreasing sequence. Then

$$d(p,q) = a_r$$

is also an ultrametric. Let us prove that it satisfies the ultrametric inequality:

Let $p, q, r \in X^\omega$ be three infinite paths. Assume that p and q coincide at exactly the first m symbols, that p and r coincide exactly at the first n symbols and that r and q coincide exactly at the first l symbols. We distinguish two cases: if $m \geq n$, since the sequence is decreasing, we have $a_m \leq a_n$, that is, $d(p,q) \leq d(p,r) \leq \max\{d(p,r), d(r,q)\}$. Otherwise, we have $m > n$. Then it follows that $m = l$ and so $d(p,q) = d(q,r) \leq \max\{d(q,r), d(p,r)\}$.

Let us describe the closed balls. Since the distance can only be a number of the form 2^{-r} it is clear that all closed balls are of the form $\overline{B}(p, 2^{-r})$ for some path $p \in X^\omega$. More precisely, these balls are formed by all the paths which coincide exactly at the first r symbols, as the red part of the following diagram shows:



Now it is clear that any two balls are either disjoint or one is included in the other. Moreover, any path included in the ball is also a center of the ball.

Definition 6.1.15. Let K be a field and $|\ |_1$ and $|\ |_2$ two absolute values. Then the two absolute values are said to be *equivalent* if they define the same topology on K, that is, if every set that is open with respect to one of the topologies is also open with respect to the other.

Lemma 6.1.16. *Let K be a field and $|\ |$ any absolute value. Then the sequence $(x^n)_{n\in\mathbb{N}}$ converges to 0 if and only if $|x| < 1$.*

Proof. By definition, the sequence $(x^n)_{n\in\mathbb{N}}$ will converge to zero when:

$$\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0,\ d(x^n, 0) = |x^n| = |x|^n < \varepsilon.$$

Taking into account that $|x|$ is a real number:

$$\lim_{n\to\infty} x^n = 0 \iff \lim_{n\to\infty} |x|^n = 0 \iff |x| < 1.$$

$\square$

Theorem 6.1.17. *Let $|\ |_1$ and $|\ |_2$ be two absolute values in a field K. The following statements are equivalent:*

(i) *$|\ |_1$ and $|\ |_2$ are equivalent.*

(ii) *For any $x \in K$ we have $|x|_1 < 1$ if and only if $|x|_2 < 1$.*

(iii) *There exists a positive real number α such that for every $x \in K$ we have:*

$$|x|_1 = |x|_2^\alpha.$$

Proof. We follow the usual method of proving a circle of implications.

$$\text{(i)} \implies \text{(ii)} \implies \text{(iii)} \implies \text{(i)}$$

(i) $\implies$ (ii). Suppose that the both absolute values define the same topology. Then taking a sequence $(x^n)_{n\in\mathbb{N}}$ which converges to zero with respect to one absolute value, it also converges with respect to the other one. According to Lemma 6.1.16 we have:

$$|x|_1 < 1 \iff \lim_{n\to\infty} x^n = 0 \iff |x|_2 < 1$$

(ii) $\implies$ (iii). Suppose that statement (ii) holds. If either $|\ |_1$ or $|\ |_2$ are the trivial absolute value, (ii) implies that the other absolute value is also the trivial one. As both are the same absolute value, taking $\alpha = 1$ statement (iii) is true.

In the general case, the statement (ii) implies this other relation:

$$|x|_1 > 1 \iff |x|_2 > 1$$
$$|x|_1 = 1 \iff |x|_2 = 1$$

This is true because in a field K with any absolute value $|\ |$, there is a one to one correspondence between the elements such that $|x| > 1$ and the elements such that $|x| < 1$ (except 0). This correspondence is given by the inverse function, which is a bijection in K^*. Hence, it suffices to prove the statement (iii) to the elements x such that $|x| \geq 1$. However, for the elements of absolute value equal to one (iii) is trivial, because the relation holds for any $\alpha \in \mathbb{R}$.

On the other hand, for all x in K there exists an unique function $\alpha\colon K \to \mathbb{R}^{>0}$ such that $|x|_1 = |x|_2^{\alpha(x)}$. It is enough to see that α does not depend on the value of x, that is, α is the constant function. In order to see that, take $x, y \in K$ such that $|x|_i, |y|_i > 1$ for $i = 1, 2$.

Fix two any $n, m \in \mathbb{N}$ such that, $|x|_1^m < |y|_1^n$. Then taking into account statement (ii).

$$|x|_1^m < |y|_1^n \iff \left|\frac{x^m}{y^n}\right|_1 < 1 \iff \left|\frac{x^m}{y^n}\right|_2 < 1 \iff |x|_2^m < |y|_2^n$$

Taking logarithms (both absolute values are greater than one),

$$m \ln|x|_1 < n \ln|y|_1 \iff m \ln|x|_2 < n \ln|y|_2$$

Since $|x|_1 = |x|_2^{\alpha(x)}$ and $|y|_1 = |y|_2^{\alpha(y)}$,

$$m\alpha(x) \ln|x|_2 < n\alpha(y) \ln|y|_2 \iff m \ln|x|_2 < n \ln|y|_2$$

and so,

$$\frac{m}{n} < \frac{\alpha(y) \ln|y|_2}{\alpha(x) \ln|x|_2} \iff \frac{m}{n} < \frac{\ln|y|_2}{\ln|x|_2}.$$

This must happen with two arbitrary natural numbers, so both values must be equal.

$$\frac{\alpha(y) \ln|y|_2}{\alpha(x) \ln|x|_2} = \frac{\ln|y|_2}{\ln|x|_2} \implies \alpha(x) = \alpha(y)$$

That is, $\alpha(x) = \alpha(y)$, $\forall x, y \neq 0 \in K$, so α must be the constant funtion. Thus, there exists $\alpha \in \mathbb{R}^{>0}$ such that $|x|_1 = |x|_2^{\alpha}$.

Finally, for $x = 0$ the statement is trivial, because, for any absolute value $|x| = 0$. Then for any $\alpha \in \mathbb{R}^{>0}$ $|0|_1 = |0|_2^{\alpha}$.

(iii) $\implies$ (i). In order to see that both absolute values define the same topology, it is enough to prove that any open ball with respect to $| \ |_2$ is also an open ball, maybe with a different radius, with respect to $| \ |_1$. In this way, the collections of all open balls will be the same.

Let $B_1 \in \tau_1$ (the topology defined by $| \ |_1$) be the ball of radius r and center $y \in K$, i.e.,

$$\begin{aligned} B_1 = \{x \in K \mid |x-y|_1 < r\} &= \{x \in K \mid |x-y|_2^{\alpha} < r\} = \\ = \{x \in K \mid |x-y|_2 < r^{\frac{1}{\alpha}}\} &= B_2(y, r^{\frac{1}{\alpha}}). \end{aligned}$$

Therefore we have the desired result. □

6.2 The valuation ring

Theorem 6.2.1. *Let K be a field with a non-archimedean absolute value, $| \ |$. Then*

(i) $\mathcal{O} = \{x \in K \mid |x| \leq 1\}$ *is a ring. This ring is called the* valuation ring.

(ii) $\mathfrak{p} = \{x \in K \mid |x| < 1\}$ *is a maximal ideal of $\mathcal{O}$. Moreover, any element x in $\mathcal{O}$ and outside $\mathfrak{p}$ is a unit in the ring $\mathcal{O}$. The ideal $\mathfrak{p}$ is called the* valuation ideal.

Proof. (i) Let K be a field, hence a ring, such that $\mathcal{O} \subseteq K$. Then it is enough to prove these three conditions:

1. For all $x, y \in \mathcal{O}$, $|x - y| \leq \max\{|x|, |-y|\} = \max\{|x|, |y|\} \leq 1$. Then $x - y \in \mathcal{O}$.

2. For all $x, y \in \mathcal{O}$, $|xy| = |x||y| \leq 1$. Then $xy \in \mathcal{O}$.

3. $|1| = 1$. Then $1 \in \mathcal{O}$.

Hence, $\mathcal{O}$ is a ring. (ii) Clearly, $\mathfrak{p}$ is a non-empty subset of $\mathcal{O}$, so in order to see that it is an ideal it suffices to prove these conditions:

1. For all $x, y \in \mathfrak{p}$, $|x + y| \leq \max\{|x|, |y|\} < 1$. Then $x + y \in \mathfrak{p}$.

2. For all $x \in \mathfrak{p}$ and $a \in \mathcal{O}$, $|ax| = |a||x| < 1$. Then $ax \in \mathfrak{p}$.

Hence, $\mathfrak{p}$ is an ideal of $\mathcal{O}$.

To see that any element x in $\mathcal{O} \setminus \mathfrak{p}$ is a unit in $\mathcal{O}$ let us take $x \in \mathcal{O} \setminus \mathfrak{p}$. Then $|x| = 1$, so $x \neq 0$ and there exists the inverse of that element, $x^{-1} \in K$. Moreover, the inverse is contained in $\mathcal{O}$; because $|x^{-1}| = \frac{1}{|x|} = 1$. Now, any ideal $\mathfrak{m}$, such that, $\mathfrak{p} \subsetneq \mathfrak{m}$ will contain a unit, so $\mathfrak{m} = \mathcal{O}$ and $\mathfrak{p}$ is a maximal ideal. $\square$

In a UFD there is another way of characterizing the valuation ring and the valuation ideal, as will be seen in the next example.

Example 6.2.2. Let A be a UFD, $p \in A$ an irreducible element and K the field of fractions of A.

Then take the p-adic valuation and the p-adic absolute value defined in Example 6.1.5. Now, the valuation ring and the valuation ideal can be described using divisibility:

$$\begin{aligned}\mathcal{O} &= \left\{\frac{a}{b} \in K \mid \left|\frac{a}{b}\right|_p \leq 1 \text{ where } \frac{a}{b} \text{ is in lowest terms}\right\} \\ &= \left\{\frac{a}{b} \in K \mid p \nmid b \text{ where } \frac{a}{b} \text{ is in lowest terms}\right\},\end{aligned}$$

Since

$$\left|\frac{a}{b}\right|_p \leq 1 \iff \nu_p\left(\frac{a}{b}\right) \geq 0 \iff \nu_p(a) - \nu_p(b) \geq 0 \iff \nu_p(a) \geq \nu_p(b).$$

If the fraction $\frac{a}{b}$ is written in lowest terms, then p can divide only one of a or b. But, if p divides b and not a, the valuation of b would be greater than the valuation of a. Hence p can not divide b in order to obtain the required inequality:

$$\left|\frac{a}{b}\right|_p \leq 1 \iff \nu_p(a) \geq \nu_p(b) \iff p \nmid b.$$

Notice that the ring $\mathcal{O}$ is A localized at the ideal (p), i.e., $\mathcal{O} = A_{(p)}$.

And,

$$\begin{aligned}\mathfrak{p} &= \left\{ \frac{a}{b} \in K \mid \left|\frac{a}{b}\right|_p < 1 \text{ where } \frac{a}{b} \text{ is in lowest terms} \right\} \\ &= \left\{ \frac{a}{b} \in K \mid p \nmid b \text{ and } p \mid a \text{ where } \frac{a}{b} \text{ is in lowest terms} \right\}\end{aligned}$$

Since

$$\left|\frac{a}{b}\right|_p < 1 \iff \nu_p\left(\frac{a}{b}\right) > 0 \iff \nu_p(a) - \nu_p(b) > 0 \iff \nu_p(a) > \nu_p(b).$$

As $\frac{a}{b}$ is written in the lowest terms, p divides only one of a or b. In order to have the inequality $\nu_p(a) \geq \nu_p(b)$ p can not divide b, and to have the strict inequality $\nu_p(a)$ must be strictly positive, i.e., p divides a. In other words,

$$\left|\frac{a}{b}\right|_p < 1 \iff \nu_p(a) > \nu_p(b) \iff p \mid a \text{ and } p \nmid b.$$

Definition 6.2.3. Let A be a ring with only one maximal ideal. Then A is called a *local ring.*

Proposition 6.2.4. *Let K be a field with a non-archimedean absolute value. Then $\mathcal{O}$ is a local ring and $\mathfrak{p}$ is its unique maximal ideal.*

Proof. We already know that $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$ and according to Theorem 6.2.1, any $x \in \mathcal{O} \smallsetminus \mathfrak{p}$ is an unit in $\mathcal{O}$. Suppose by contradiction that $\mathfrak{m}$ is a different maximal ideal of $\mathcal{O}$. Then $\mathfrak{m}$ can not be contained in a proper ideal of $\mathcal{O}$, and in particular is not contained in $\mathfrak{p}$. Since

$$\mathfrak{m} \nsubseteq \mathfrak{p} \implies \exists y \in \mathfrak{m} \smallsetminus \mathfrak{p} \subseteq \mathcal{O} \smallsetminus \mathfrak{p},$$

$\mathfrak{m}$ contains a unit in $\mathcal{O}$, so $\mathfrak{m} = \mathcal{O}$ which is a contradiction, because $\mathfrak{m}$ must be a proper ideal. Thus the unique maximal ideal of $\mathcal{O}$ is $\mathfrak{p}$. $\square$

Now, $\mathfrak{p}$ is a maximal ideal of the ring $\mathcal{O}$, so $\mathcal{O}/\mathfrak{p}$ is a field, which is called the *residue field.* Let us analyze the residue field in three particular cases.

Examples 6.2.5. (1) The p-adic valuation in $\mathbb{Q}$ (p being a prime number). $\mathbb{Q}$ is the field of fractions of the UFD $\mathbb{Z}$. So according to Example 6.2.2:

$$\mathcal{O} = \mathbb{Z}_{(p)},$$

$$\mathfrak{p} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \text{ and } p \mid a \right\} = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} \mid p \mid a \right\} = p\mathbb{Z}_{(p)}.$$

Finally, the residue field is given by this isomorphism:

$$\frac{\mathcal{O}}{\mathfrak{p}} = \frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \cong \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p$$

To prove the isomorphism we define the following map φ and use the First Isomorphism Theorem:

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z}_{(p)} & \to & \mathbb{F}_p \\ & \frac{a}{b} & \mapsto & \varphi\left(\frac{a}{b}\right) = \overline{a} \cdot \overline{b}^{-1}. \end{array}$$

Since the fraction is written in lowest terms there is a unique representation of the elements of $\mathbb{Z}_{(p)}$. And $\frac{a}{b} \in \mathbb{Z}_{(p)}$, so p does not divide b and $\overline{b} \neq \overline{0}$, thus writing $\overline{b}^{-1}$ makes sense. Hence, the function φ is well-defined.

Moreover, φ is ring homomorphism, because it has the three required properties:

1. Firstly,

$$\begin{aligned} \varphi\left(\frac{a}{b} + \frac{c}{d}\right) &= \varphi\left(\frac{ad+bc}{bd}\right) = \overline{ad+bc} \cdot \overline{bd}^{-1} \\ &= \overline{a} \cdot \overline{b}^{-1} + \overline{c} \cdot \overline{d}^{-1} = \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right). \end{aligned}$$

2. Moreover,

$$\varphi\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \overline{ac} \cdot \overline{bd}^{-1} = (\overline{a} \cdot \overline{b}^{-1}) \cdot (\overline{c} \cdot \overline{d}^{-1}) = \varphi\left(\frac{a}{b}\right) \cdot \varphi\left(\frac{c}{d}\right).$$

3. Finally, $\varphi(1) = \overline{1}$.

Obviously, φ is onto; i.e. $\operatorname{im}\varphi = \mathbb{F}_p$ because

$$\varphi(a) = \varphi\left(\frac{a}{1}\right) = \overline{a},\ \forall\, \overline{a} \in \mathbb{F}_p.$$

Finally, the kernel of the homomorphism is

$$\begin{aligned} \ker\varphi &= \left\{\frac{a}{b} \in \mathbb{Z}_{(p)} \mid \varphi\left(\frac{a}{b}\right) = \overline{0}\right\} = \left\{\frac{a}{b} \in \mathbb{Z}_{(p)} \mid \overline{a} = \overline{0}\right\} \\ &= \left\{\frac{a}{b} \in \mathbb{Z}_{(p)} \mid p \mid a\right\} = p\mathbb{Z}_{(p)}. \end{aligned}$$

Furthermore, according to the First Isomorphism Theorem, we obtain the required isomorphism:

$$\frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \cong \mathbb{F}_p.$$

(2) The $p(t)$-adic valuation in $F(t)$ (being $p(t)$ an irreducible polynomial).

Let $F(t)$ be the field of fractions of the UFD $F[t]$, so this is another particular case of Example 6.2.2. Reproducing the previous argument, the residue field of $| \ |_{p(t)}$ is given by the next isomorphism:

$$\frac{F[t]_{(p(t))}}{p(t)F[t]_{(p(t))}} \cong \frac{F[t]}{(p(t))}.$$

In general, the residue field is a finite extension of F, and in some particular cases it is very well-known. For example, when F is the complex field, $F = \mathbb{C}$, then $p(t)$ is any polynomial of degree one, for example $p(t) = t - \alpha$, the residue field is $\mathbb{C}$, because of this isomorphism:

$$\frac{\mathbb{C}[t]}{(p(t))} \cong \mathbb{C}.$$

(3) In a more general context, let A be a PID, K its field of quotients and consider the p-adic absolute value, $| \ |_p$, corresponding to an irreducible element $p \in A$. Then the residue field of $| \ |_p$ is described by the isomorphism:

$$\frac{A_{(p)}}{pA_{(p)}} \cong \frac{A}{pA}.$$

6.3 Cauchy sequences

Definition 6.3.1. Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in a field K with respect to an absolute value $| \ |$. Then $(x_n)_{n\in\mathbb{N}}$ is said to be a *Cauchy sequence* when:

$$\forall \varepsilon > 0 \ \ \exists \ n_0 \in \mathbb{N} \text{ such that } \forall m, n > n_0 \ |x_m - x_n| < \varepsilon.$$

Proposition 6.3.2. *Let $(x_n)_{n\in\mathbb{N}}$ be a convergent sequence in a field K with respect to an absolute value $| \ |$. Then $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence.*

Lemma 6.3.3. *Let K be a field and $| \ |$ a non-archimedean absolute value. If*

$$\forall \varepsilon > 0 \ \ \exists \ n_0 \in \mathbb{N} \textit{ such that } \forall n > n_0 \ \ |x_{n+1} - x_n| < \varepsilon.$$

Then $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence.

Proof. By hypothesis:

$$\forall \varepsilon > 0 \ \ \exists n_0 \in \mathbb{N} \text{ such that } \forall n > n_0 \ \ |x_{n+1} - x_n| < \varepsilon.$$

Take any $m, n > n_0$. As the absolute value is non-archimedean,

$$\begin{aligned} |x_m - x_n| &= |x_m - x_{m-1} + x_{m-1} - x_{m-2} + \cdots + x_i - x_{i-1} + \cdots + x_{n+1} - x_n| \\ &\leq \ \max\{|x_m - x_{m-1}|, \ldots, |x_{n+1} - x_n|\} = |x_{n_1+1} - x_{n_1}|, \end{aligned}$$

for some $n_1 > n_0$. Hence, $|x_{n_1+1} - x_{n_1}| < \varepsilon$ and

$$\forall \varepsilon > 0 \ \exists n_0 \in \mathbb{N} \text{ such that } \forall m, n > n_0 \ \ |x_m - x_n| \leq |x_{n_1+1} - x_{n_1}| < \varepsilon.$$

Thus, $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence. $\square$

Obviously, the inverse of this result is true with respect to any absolute value, so the lemma gives us another characterization of Cauchy sequences with respect to non-archimedean absolute values. Moreover, the property holds in any ultrametric space.

However, its is generally false for archimedean absolute values. As a counter-example consider the next statement:

Example 6.3.4. Consider $\mathbb{R}$ with the usual absolute value. The series $\sum_{n=1}^{\infty} \frac{1}{n}$ is divergent, so the sequence of partial sums, $(S_n)_{n\in\mathbb{N}}$ is not convergent, and since $(\mathbb{R}, d_u)$ is a complete metric space, it is neither Cauchy. This sequence is given by:

$$S_n = \sum_{k=1}^{n} \frac{1}{k}.$$

However, the weaker property holds:

$$\lim_{n\to\infty} |S_{n+1} - S_n| = \lim_{n\to\infty} \frac{1}{n+1} = 0.$$

6.3.1 Cauchy sequences and algebraic structures

Lemma 6.3.5. *Let $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ be Cauchy sequences of elements in a field K with respect to the absolute value $|\ |$. Then*

(i) $(x_n + y_n)_{n\in\mathbb{N}}$ *is a Cauchy sequence.*

(ii) $(x_n \cdot y_n)_{n\in\mathbb{N}}$ *is a Cauchy sequence.*

(iii) *If $x_n \neq 0$ for all $n \in \mathbb{N}$, then $\left(\frac{1}{x_n}\right)_{n\in\mathbb{N}}$ is a Cauchy sequence.*

Proof. It is an elementary result of Calculus. As an example, here will be proved only the first statement, the other proofs are similar. Since $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ are Cauchy sequences, for all $\varepsilon > 0$:

$$\exists n_1 \in \mathbb{N} \text{ such that } \forall m, n > n_1 \ |x_m - x_n| < \frac{\varepsilon}{2},$$

$$\exists n_2 \in \mathbb{N} \text{ such that } \forall m, n > n_2 \ |y_m - y_n| < \frac{\varepsilon}{2}.$$

Now, choose $n_0 = \max\{n_1, n_2\}$. Then for all $m, n > n_0$

$$|(x+y)_m - (x+y)_n| = |x_m - x_n - (y_n - y_m)| \leq |x_m - x_n| + |y_m - y_n| < \varepsilon.$$

Hence, $((x+y)_n)_{n\in\mathbb{N}}$ is Cauchy. □

Lemma 6.3.6. *Let K be a field with an absolute value $|\ |$. Then*

$$\mathcal{C} = \{(a_n)_{n\in\mathbb{N}} \mid (a_n)_{n\in\mathbb{N}} \textit{ is a Cauchy sequence of elements in } K\}$$

is a ring with respect to the componentwise addition and multiplication.

Proof. $\mathcal{C}$ is a subset of the set of sequences with elements in K, $K^{\mathbb{N}}$, which is a ring. Hence, in order to see that $\mathcal{C}$ is a subring it is enough to prove this three conditions. The first two conditions are consequences of Lemma 6.3.5.

1. For all $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}} \in \mathcal{C}$, $(a_n)_{n\in\mathbb{N}} - (b_n)_{n\in\mathbb{N}} \in \mathcal{C}$.
2. For all $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}} \in \mathcal{C}$, $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} \in \mathcal{C}$.
3. All the constant sequences are convergent. In particular, they are Cauchy sequences, so $(1)_{n\in\mathbb{N}} \in \mathcal{C}$.

□

Lemma 6.3.7. *Let K be a field with an absolute value $|\ |$. Then*

$\mathfrak{m} = \{(a_n)_{n\in\mathbb{N}} \mid (a_n)_{n\in\mathbb{N}}$ *is a sequence with elements in K that converges to zero*$\}$

is a maximal ideal of $\mathcal{C}$.

Proof. Firstly, we shall see that $\mathfrak{m}$ is an ideal. Obviously, is a non empty set contained in $\mathcal{C}$ (all the convergent sequences are Cauchy sequences). For example, the constant zero sequence is convergent to zero, thus Cauchy; so it is contained in $\mathfrak{m}$. Hence, it is enough to check this two conditions.

1. For all $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}} \in \mathfrak{m}$, $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} \in \mathfrak{m}$.
The sum of two convergent sequences is also convergent and its limit is just the sum of the limits, which in this case is zero. Then $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}}$ converges to zero, so is contained in $\mathfrak{m}$.

2. For all $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}$ and $(b_n)_{n\in\mathbb{N}} \in \mathfrak{m}$, $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} \in \mathfrak{m}$.
By elementary calculus we know that any Cauchy sequence is bounded, in particular $(a_n)_{n\in\mathbb{N}}$. That is, there exists $M > 0$ such that $|a_n| < M$, for all $n \in \mathbb{N}$. Moreover, $(b_n)_{n\in\mathbb{N}} \in \mathfrak{m}$ is convergent to zero, i.e.

$$\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N} \text{ such that } \forall n > n_0\ |b_n| < \frac{\varepsilon}{M}.$$

Then for that $\varepsilon > 0$ and for any $n > n_0$:

$$|a_n \cdot b_n| = |a_n| \cdot |b_n| < M\frac{\varepsilon}{M} = \varepsilon.$$

And, $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}}$ is convergent to zero.

Secondly, to see that $\mathfrak{m}$ is a maximal ideal, we will prove that $\mathfrak{a} := \mathfrak{m} + (a) = \mathcal{C}$, for any element a in $\mathcal{C} \setminus \mathfrak{m}$.

Therefore, $a = (x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence which does not converge to zero, so $x_n \neq 0$ except for a finite number of values. Then we can define the sequence $(y_n)_{n\in\mathbb{N}}$ such that

$$y_n = \begin{cases} 0 & \text{if } x_n \neq 0 \\ 1 & \text{if } x_n = 0. \end{cases}$$

Then $(y_n)_{n\in\mathbb{N}}$ is a semiconstant sequence, with value zero except for a finite number of indexes. Hence it is convergent to zero, that is, $(y_n)_{n\in\mathbb{N}} \in \mathfrak{m} \subseteq \mathfrak{a}$. Hence,

$$(y_n)_{n\in\mathbb{N}}, (x_n)_{n\in\mathbb{N}} \in \mathfrak{a} \implies (z_n)_{n\in\mathbb{N}} = (x_n + y_n)_{n\in\mathbb{N}} \in \mathfrak{a}.$$

Besides, $z_n \neq 0$, for all $n \in \mathbb{N}$. Therefore, $\left(\frac{1}{z_n}\right)_{n\in\mathbb{N}}$ is a well-defined sequence (all the terms are non zero) and according to Lemma 6.3.5 it is a Cauchy sequence. Then

$$\left(\tfrac{1}{z_n}\right)_{n\in\mathbb{N}} \in \mathcal{C} \text{ and } (z_n)_{n\in\mathbb{N}} \in \mathfrak{a} \implies \left(z_n \cdot \tfrac{1}{z_n}\right)_{n\in\mathbb{N}} = (1)_{n\in\mathbb{N}} \in \mathfrak{a}.$$

Finally, since the identity is contained in $\mathfrak{a}$, it is the total ring $\mathcal{C}$ and $\mathfrak{m}$ is a maximal ideal. □

Hence, we have got a ring and a maximal ideal, it is natural to define the quotient field, $\hat{K} = \mathcal{C}/\mathfrak{m}$ and there is also a intuitive way to construct an absolute value on $\hat{K}$, starting from the absolute value on K. We should prove one before define the absolute value.

Lemma 6.3.8. *Let K be a field with a non-archimedean absolute value $|\ |$ and let $(x_n)_{n\in\mathbb{N}}$ be a Cauchy sequence not converging to zero. (i.e. $(x_n)_{n\in\mathbb{N}} \in \mathcal{C}\setminus\mathfrak{m}$). Then the sequence $(|x_n|)_{n\in\mathbb{N}}$ is eventually stationary, that is,*

$$\exists n_0 \in \mathbb{N} \textit{ such that } |x_n| = |x_{n_0}| \ \forall n \geq n_0.$$

Proof. On the one hand, the sequence $(x_n)_{n\in\mathbb{N}}$ does not converge to zero, then there exists a real number $c > 0$ and $n_1 \in \mathbb{N}$ such that

$$d(x_n, 0) = |x_n| > c, \ \ \forall n \geq n_1.$$

On the other hand, $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence, so

$$\exists n_2 \in \mathbb{N} \text{ such that } |x_n - x_m| < c, \ \ \forall m, n \geq n_2.$$

Hence, put $n_0 = \max\{n_1, n_2\}$ and take any $n > n_0$. Then for these values:

$$|x_n|, \ |x_{n_0}| > c \text{ and } |x_n - x_{n_0}| < c.$$

Then we can construct a triangle whose edges have lengths, $|x_n|, |x_{n_0}|$ and $|x_n - x_{n_0}|$. According to Proposition 6.1.13 the triangle is isosceles, and the two longest sides ($|x_n|$ and $|x_{n_0}|$), have the same lenght. That is,

$$|x_n| = |x_{n_0}| \ \forall n > n_0$$

and the sequence $(|x_n|)_{n\in\mathbb{N}}$ is eventually constant. □

Proposition 6.3.9. *Let K be a field with respect to the non-archimedean absolute value $|\ |$. If x is an element of the field $\hat{K} = \mathcal{C} \smallsetminus \mathfrak{m}$, representative of the sequence $(x_n)_{n\in\mathbb{N}}$ with elements in K; $|\ |_\wedge$ is defined by*

$$|x|_\wedge = \lim_{n\to\infty} |x_n|.$$

Then $|\ |_\wedge$ is a well-defined absolute value on the field $\hat{K}$ and the set of values taken by $|\ |_\wedge$ is the same as the set of values taken by $|\ |$.

Proof. In order to have a well-defined absolute value, the image must always exist and be independent to the chosen representative.

According to Lemma 6.3.8 the sequence $(|x_n|)_{n\in\mathbb{N}}$ is eventually stationary, thus it is convergent and the limit exists in any case. Furthermore, since the sequence is eventually constant, the set of values of $|\ |_\wedge$ and $|\ |$ coincide.

Futhermore, the limit does not depend on the representative itself. Let $(x_n)_{n\in\mathbb{N}}$ and $(\overline{x}_n)_{n\in\mathbb{N}}$ be sequences representing x. Then

$$(x_n)_{n\in\mathbb{N}} \sim (\overline{x}_n)_{n\in\mathbb{N}} \implies \lim_{n\to\infty} |x_n - \overline{x}_n| = 0.$$

Thus,

$$\forall \varepsilon > 0 \ \ \exists n_0 \in \mathbb{N} \text{ such that } ||x_n| - |\overline{x}_n|| \leq |x_n - \overline{x}_n| < \varepsilon, \forall n \geq n_0 \implies$$

$$\lim_{n\to\infty} ||x_n| - |\overline{x}_n|| = 0 \implies \lim_{n\to\infty} |x_n| = \lim_{n\to\infty} |\overline{x}_n|.$$

Therefore, the function $|\ |_\wedge$ is well defined and it is also a non-archimedean absolute value, since it holds the three conditions of the characterization:

1. Since the absolute value is independent of the representative itself, it is enough to choose any sequence contained in $\mathfrak{m}$ which representates 0. For example, the constant sequence $(0)_{n\in\mathbb{N}}$. Thus, $|0|_\wedge = \lim_{n\to\infty}|0| = 0$.
2. For all $x, y \in \hat{K}$,
$$|xy|_\wedge = \lim_{n\to\infty} |xy| = \lim_{n\to\infty} |x| \lim_{n\to\infty} |y| = |x|_\wedge |y|_\wedge.$$
3. For all $x, y \in \hat{K}$,
$$\begin{aligned} |x+y|_\wedge = \lim_{n\to\infty} |x+y| \leq \lim_{n\to\infty} \max\{|x| + |y|\} = \max\{\lim_{n\to\infty} |x| + \lim_{n\to\infty} |y|\} \\ = \max\{|x|_\wedge + |y|_\wedge\} \end{aligned}$$

The last two conditions hold because of the properties of the limit.

□

6.4 Completions

The property of non-archimedean absolute values described in Lemma 6.3.3 gives us a strong criterion to evaluate the convergence of series. One necessary condition for convergence in elementary calculus will become also sufficient when we are working in complete fields with respect to non-archimedean absolute values.

Proposition 6.4.1. *Let K be a complete field with respect to a non-archimedean absolute value $|\ |$. Then a series is convergent if and only if the general term converges to zero. That is,*

$$\sum_{n=1}^{\infty} x_n < \infty \iff \lim_{n\to\infty} x_n = 0.$$

Proof. $\Rightarrow$) As $\sum_{n=1}^{\infty} x_n$ is convergent the sequence of partial sums $(S_n)_{n\in\mathbb{N}}$ is also convergent. Let $S = \lim_{n\to\infty} S_n$.

For all $n \geq 2$, $x_n = S_n - S_{n-1}$. Then

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} (S_n - S_{n-1}) = \lim_{n\to\infty} S_n - \lim_{n\to\infty} S_{n-1} = S - S = 0.$$

$\Leftarrow$) Being $(S_n)_{n\in\mathbb{N}}$ the sequence of partial sums, for all $n \geq 2$, $x_n = S_n - S_{n-1}$. Then:

$$\lim_{n\to\infty} (S_n - S_{n-1}) = \lim_{n\to\infty} x_n = 0 \implies \lim_{n\to\infty} |S_n - S_{n-1}| = 0.$$

According to Lemma 6.3.3 the sequence $(S_n)_{n\in\mathbb{N}}$ is Cauchy. Finally, as the space is complete $(S_n)_{n\in\mathbb{N}}$ is also convergent, so the series is convergent. $\square$

The reader can appreciate how useful it is working with non-archimedean absolute values. Sadly, in most cases we do not work in this context.

Definition 6.4.2. Let K be a field with an absolute value. A *completion* of K is a field $\hat{K}$ with an an absolute value $|\ |_\wedge$ containing K such that:

(i) $|x|_\wedge = |x|$ for all $x \in K$.

(ii) $\hat{K}$ is complete.

(iii) K is dense in $\hat{K}$.

The following theorem guarantees us the existence of such completion field. Firstly, recall the following lemma from Topology:

Lemma 6.4.3. *Let (X, τ_X) and (Y, τ_Y) two topological spaces, such that, (Y, τ_Y) is Hausdorff, D a dense subset of X and two continuous functions $f, g\colon (X, \tau_X) \to (Y, \tau_Y)$, such that $f(x) = g(x)$ for all $x \in D$. Then $f = g$.*

Theorem 6.4.4. *For each field K with respect to the non-archimedean absolute value $| \ |$ there exists a field $\hat{K}$ with a non-archimedean absolute value $| \ |_\wedge$, such that:*

(i) *there exists an inclusion $K \subseteq \hat{K}$ and the absolute value induced by $| \ |_\wedge$ in K via this inclusion is $| \ |$.*

(ii) *the image of K under this inclusion is dense in $\hat{K}$ (with respect to the absolute value $| \ |_\wedge$).*

(iii) *$\hat{K}$ is complete with respect to the absolute value $| \ |_\wedge$.*

The field $\hat{K}$ satisfying (i), (ii) *and* (iii) *is unique up to unique K-isomorphism preserving the absolute values.*

Proof. The field in which K will be embedded, $\hat{K}$, is the quotient field, $\mathcal{C}/\mathfrak{m}$ where $\mathcal{C}$ is the ring of Cauchy sequences of elements in K and $\mathfrak{m}$ the maximal ideal of sequences which converge to zero.

(i) We will prove that K is embedded in $\hat{K}$ by the mapping: $\varphi : K \to \hat{K}$ such that $\varphi(x) = (x)_{n\in\mathbb{N}} + \mathfrak{m}$. Then φ is a ring monomorphism. We shall first prove that φ is a homomorphism. As the addition and multiplication are defined componentwise, the first two conditions are obvious.

1. $\varphi(a) + \varphi(b) = (a)_{n\in\mathbb{N}} + \mathfrak{m} + (b)_{n\in\mathbb{N}} + \mathfrak{m} = (a + b)_{n\in\mathbb{N}} + \mathfrak{m} = \varphi(a + b)$.
2. $\varphi(a)\varphi(b) = ((a)_{n\in\mathbb{N}} + \mathfrak{m}) \cdot ((b)_{n\in\mathbb{N}} + \mathfrak{m}) = (ab)_{n\in\mathbb{N}} + \mathfrak{m} = \varphi(ab)$.
3. $\varphi(1) = (1)_{n\in\mathbb{N}}$.

While we are seeing that φ is well defined we also prove that φ is injective:

$$\varphi(a) = \varphi(b) \iff (a)_{n\in\mathbb{N}} + \mathfrak{m} = (b)_{n\in\mathbb{N}} + \mathfrak{m} \iff (a - b)_{n\in\mathbb{N}} \in \mathfrak{m}.$$

Thus, $(a - b)_{n\in\mathbb{N}}$ is a constant convergent sequence, whose limit is zero, that is, it must be the constant zero sequence. So $a - b = 0$ and $a = b$, as required. Therefore, φ is well-defined and it is a monomorphism.

Finally, by the First Isomorphism Theorem:

$$\frac{K}{\ker\varphi} \cong \mathrm{im}\varphi \implies K \cong \mathrm{im}\varphi \leq \hat{K}.$$

Therefore, K is isomorphic to a subfield of $\hat{K}$, hence K is embedded in $\hat{K}$.

Finally, we shall see that the absolute value $| \ |_\wedge$ in $\hat{K}$ via this inclusion is the absolute value $|\ |$ on K. That is, we shall see that $|x| = |\varphi(x)|_\wedge$ for all x in K. It is true since

$$|\varphi(x)|_\wedge = |(x)_{n\in\mathbb{N}} + \mathfrak{m}|_\wedge = \lim_{n\to\infty} |x| = |x|.$$

(ii) We shall see that any open ball around an element $\lambda \in \hat{K}$ contains an element of (the image of) K, i.e., a equivalence class of a constant sequence. So fix a radius ε and build the ball $B(\lambda, \varepsilon)$.

Let $(x_n)_{n\in\mathbb{N}}$ be a Cauchy sequence representing λ, and let ε' be a number slightly smaller than ε. By the Cauchy property, there exists a natural number N such that $|x_n - x_m| < \varepsilon'$ whenever $n, m \geq N$. Let $y = x_N$ and consider the constant sequence $(y)_{n\in\mathbb{N}}$.

Recall that $\lambda - y$ is represented by the sequence $(x_n - y)_{n\in\mathbb{N}}$, and the absolute value is defined as:

$$|\lambda - (y)_{n\in\mathbb{N}}|_\wedge = \lim_{n\to\infty} |x_n - y|.$$

But, whenever $n \geq N$:

$$|x_n - y| = |x_n - x_N| < \varepsilon'.$$

So in the limit we have:

$$|\lambda - (y)_{n\in\mathbb{N}}|_\wedge = \lim_{n\to\infty} |x_n - y| \leq \varepsilon' < \varepsilon \implies (y)_{n\in\mathbb{N}} \in B(\lambda, \varepsilon).$$

Therefore, the constant sequence $(y)_{n\in\mathbb{N}}$ belongs to $B(\lambda, \varepsilon)$ as required. Hence, the image of K is dense in $\hat{K}$.

(iii) We shall see that any Cauchy sequence is convergent with respect to $|\ |_\wedge$.

Let $(\Lambda_n)_{n\in\mathbb{N}}$ be a Cauchy sequence of elements in $\hat{K}$, (so each $\Lambda_n = (\lambda_i)_{i\in\mathbb{N}} + \mathfrak{m}$ is the residue class of a Cauchy sequence of elements in K). According to statement (ii) the image of K is dense in $\hat{K}$. Thus, for any Λ_n in $\hat{K}$ there exists an element of K, say $y^{(n)}$, such that, the constant sequence $\Lambda'_n = (y^{(n)})_{k\in\mathbb{N}} + \mathfrak{m}$ is contained in the ball of center Λ_n and radius $\frac{1}{n}$, i.e.,

$$0 = \lim_{n\to\infty} |\Lambda_n - \Lambda'_n|_\wedge = \lim_{n\to\infty} |\lambda_n - y^{(n)}|.$$

Hence, consider the sequence $B = (y^{(n)})_{n\in\mathbb{N}}$ with elements in K. This sequence is a Cauchy sequence. Since the previous limit holds,

$$\forall\varepsilon > 0,\ \exists n_0 \in \mathbb{N} \text{ such that } |\lambda_n - y^{(n)}| < \frac{\varepsilon}{2},\ \forall n \geq n_0.$$

Then

$$|y^{(n+1)} - y^{(n)}| = |y^{(n+1)} - \lambda_n + \lambda_n - y^{(n)}| \leq |y^{(n+1)} - \lambda_n| + |\lambda_n - y^{(n)}| < \varepsilon,\ \forall n \geq n_0.$$

Hence, according to Lemma 6.3.3, $(y^{(n)})_{n\in\mathbb{N}}$ is a Cauchy sequence in K, and consider $A = \varphi\left((y^{(n)})_{n\in\mathbb{N}}\right) = (y^{(n)})_{n\in\mathbb{N}} + \mathfrak{m}$.

Now, notice that

$$|\Lambda_n - A|_\wedge = |(\lambda_n)_{n\in\mathbb{N}} + \mathfrak{m} - (y^{(n)})_{n\in\mathbb{N}} + \mathfrak{m}|_\wedge$$
$$= |(\lambda_n - y^{(n)})_{n\in\mathbb{N}} + \mathfrak{m}|_\wedge = \lim_{n\to\infty} |\lambda_n - y^{(n)}| = 0.$$

Hence,

$$\lim_{n\to\infty} \Lambda_n = A.$$

Therefore, any Cauchy sequence is convergent.

Finally, we shall prove the uniqueness up to unique isomorphism preserving the absolute value. Suppose by contradiction that we have another field $\overline{K}$ satisfying the same properties. Then we can think of the inclusion $K \subseteq \overline{K}$ as a map defined on a dense subset of $\hat{K}$. This map has to preseve the absolute values of any element of K, it is continuous:

$$\forall \varepsilon > 0 \ \exists \delta = \varepsilon > 0 \text{ such that } 0 < |x-y| < \delta \implies |\psi(x) - \psi(y)|_\wedge = |x-y| < \varepsilon.$$

Now, any map defined on a dense subset which is continuous can be extended uniquely to the whole field, so that we get a map $\Psi\colon \hat{K} \to \overline{K}$ which is the unique continuous extension of the inclusion of K in $\overline{K}$. It is now easy to check that Ψ is an isomorphism that preserves the absolute values.

The inclusion preserves the operations on K and these operations are continuous. Thus, the extended map also preserves the addition and the multiplication. Here we are proving that multiplication is preserved (the addition is proved in the same way). Consider the functions $\Phi_1\colon \hat{K}\times\hat{K} \to \overline{K}$ such that $\Phi_1(x,y) = \Psi(xy)$ and $\Phi_2\colon \hat{K}\times\hat{K} \to \overline{K}$ such that $\Phi_2(x,y) = \Psi(x)\Psi(y)$. Futhermore, $K \times K$ is dense in $\hat{K}\times\hat{K}$ and $\overline{K}$ is Hausdorff with respect the induced metric, because it is a metrizable topological space. Hence, according to Lema 6.4.3:

$$\Phi_1(x,y) = \Psi(xy) = \Psi(x)\Psi(y) = \Phi_2(x,y) \quad \forall (x,y) \in K\times K$$
$$\implies \Phi_1 \equiv \Phi_2 \implies \Psi(xy) = \Psi(x)\Psi(y) \quad \forall (x,y) \in \hat{K}\times\hat{K}.$$

Therefore as both operations are preserved, Ψ is a homomorphism of fields and thus it is injective.

Performing the same construction in the reverse to get the opposite direction, we get the field homomorphism $\Psi_2\colon \overline{K} \to \hat{K}$. Since, both are K-monomorphisms, the composition, $\Psi\circ\Psi_2\colon \hat{K} \to \hat{K}$, is a continuous map whose restriction to K is the identity, a dense subset of $\hat{K}$. Moreover, $\hat{K}$ is a metrizable space with respect the induced metric, hence it is Hausdorff. Thus, according to Lemma 6.4.3.

$$\Psi\circ\Psi_2(x) = x = \mathrm{id}(x) \quad \forall x \in K \implies \Psi\circ\Psi_2 = \mathrm{id}_{\hat{K}}.$$

Reproducing the same argument in the reverse way, we get $\Psi_2 \circ \Psi = \mathrm{id}_{\overline{K}}$. So, $\Psi_2 = \Psi^{-1}$. Therefore, Ψ is a K-isomorphism.

Furthermore, the absolute value itself is a continuous function which is preserved when Ψ is restricted to K, a dense subset of $\hat{K}$ which is a T_2 space with respect to the induced metric. Finally, according to Lemma 6.4.3, Ψ preserves the absolute values in $\hat{K}$. Finally, its uniqueness is clear by construction. $\square$

Remark. Notice that the completion is unique up to unique isomorphism; not unique up to isomorphism. That means, that given two different completions of the same field, there exists just one isomorphism from one to the another.

Reproducing the proof of Theorem 6.4.4 the p-adic numbers can be interpreted as a quotient field,

$$\mathbb{Q}_p = \frac{\mathcal{C}}{\mathfrak{m}},$$

where $\mathcal{C}$ are the Cauchy sequences over $\mathbb{Q}$ and $\mathfrak{m}$ the ideal of sequences over $\mathbb{Q}$ which converge to zero.

Finally, we are able to define p-adic numbers.

Definition 6.4.5. The *field of p-adic numbers*, denoted by $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value.

We may slightly change our notation for the p-adic absolute value:

Notation. We will still write $| \ |_p$ (instead of $| \ |_\wedge$) for the extension of the p-adic absolute value to $\mathbb{Q}_p$.

According to Proposition 6.3.9, the set of values of the p-adic absolute value defined in $\mathbb{Q}_p$ is the same as the set of values taken in $\mathbb{Q}$. Hence, the possible values are p^n for $n \in \mathbb{Z}$, together with the value 0.

Once that we have the p-adic absolute value defined in $\mathbb{Q}_p$, it is easy to define a valuation in $\mathbb{Q}_p$. Indeed,

$$\nu_p(x) = -\log_p |x|_p$$

is a valuation.

We have already defined the p-adic numbers. Unfortunately, the construction is rather confusing and not very intuitive. In fact, until now, p-adic numbers are equivalence classes of Cauchy sequences, which does not help much to understand them. Hence, we will be interested in finding alternative representations of the elements in $\mathbb{Q}_p$ in order to ease understading. The next section is devoted to do so. We will find some similarities between the fields $\mathbb{Q}_p$ (completion of $\mathbb{Q}$ with respect to the p-adic absolute value) and $\mathbb{R}$ (completion of $\mathbb{Q}$ with respect to the usual absolute value).

6.5 Exploring $\mathbb{Q}_p$

First we introduce some new notation for the particular case of p-adic absolute values.

Recall that given a field K with a non-archimedean absolute value $|\ |$, we have the valuation ring

$$\mathcal{O} = \{x \in K \mid |x| \leq 1\} = \overline{B}(0, 1)$$

and the valuation ideal

$$\mathfrak{p} = \{x \in K \mid |x| < 1\} = B(0, 1)$$

which is indeed the unique maximal ideal of $\mathcal{O}$.

In the case of the field $\mathbb{Q}_p$ with the p-adic absolute value, we shall write $\mathcal{O} = \mathbb{Z}_p$ and we say that $\mathbb{Z}_p$ is the *ring of p-adic integers*. The following three lemmas give us information concerning the ideals of $\mathbb{Z}_p$.

Lemma 6.5.1. *The valuation ideal of the field $\mathbb{Q}_p$ with the p-adic absolute value is*

$$\mathfrak{p} = p\mathbb{Z}_p = \overline{B}\left(0, \frac{1}{p}\right).$$

Proof. Since the only values taken by $|\ |_p$ are p^n with $n \in \mathbb{Z}$ and 0, we have $|x|_p < 1$ if and only if $|x|_p \leq \frac{1}{p}$ (if and only if $x \in \overline{B}\left(0, \frac{1}{p}\right)$, and the second equality is proved). Moreover,

$$|x|_p \leq \frac{1}{p} \iff p|x|_p \leq 1 \iff \left|\frac{1}{p}x\right|_p \leq 1 \iff \frac{1}{p}x \in \mathbb{Z}_p \iff x \in p\mathbb{Z}_p.$$

$\square$

Just like in the general case, the field, the valuation ring and the valuation ideal form a chain.

$$\begin{array}{c} \mathbb{Q}_p \\ | \\ \mathbb{Z}_p \\ | \\ p\mathbb{Z}_p \end{array}$$

The next lemma describes the principal ideals of $\mathbb{Z}_p$.

Lemma 6.5.2. *Let $x \in \mathbb{Z}_p$ with $x \neq 0$. Then there exists $n \geq 0$ such that*

$$(x) = p^n \mathbb{Z}_p.$$

Proof. Let $x \neq 0$ in $\mathbb{Z}_p$. Then since $x \neq 0$, we have $|x|_p = p^{-n}$ for some integer n. Moreover, since $|x|_p \leq 1$, it follows that $n \geq 0$. Then

$$|x|_p = p^{-n} \iff \left|\frac{1}{p^n}x\right|_p = 1 \iff \frac{1}{p^n}x = u$$

for some unit u in $\mathbb{Z}_p$. Then $x = up^n$ and so the ideals generated by x and p^n are the same, i.e. $(x) = (p^n) = p^n\mathbb{Z}_p$. $\square$

Finally, we analyze the case of an arbitrary ideal.

Lemma 6.5.3. *Let $\mathfrak{a}$ be an ideal of $\mathbb{Z}_p$. Then $\mathfrak{a} = \{0\}$ or $\mathfrak{a} = p^n\mathbb{Z}_p$ for some $n \geq 0$.*

Proof. Let $\mathfrak{a} \neq \{0\}$ be an ideal of $\mathbb{Z}_p$. Then

$$\mathfrak{a} = \sum_{x \in \mathfrak{a} \setminus \{0\}} (x)$$

and by the previous lemma,

$$\mathfrak{a} = \sum_{x \in \mathfrak{a} \setminus \{0\}} p^{n(x)}\mathbb{Z}_p.$$

Now, all the ideals $p^{n(x)}\mathbb{Z}_p$ are linearly ordered by inclusion, and so the sum of all of them is nothing but the biggest one. More specifically, taking

$$n = \min\{n(x) \mid x \in \mathfrak{a} \setminus \{0\}\},$$

we have $\mathfrak{a} = p^n\mathbb{Z}_p$. $\square$

The last lemma that we have proved gives us the following direct corollary:

Corollary 6.5.4. *The ring of p-adic integers $\mathbb{Z}_p$ is a PID.*

Hence, by Lemma 6.5.3 the ideals of $\mathbb{Z}_p$ are linearly ordered:

$$\begin{tikzcd}
\mathbb{Q}_p \arrow[d, dash] \\
\mathbb{Z}_p \arrow[d, dash] \\
p\mathbb{Z}_p \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
p^n\mathbb{Z}_p \arrow[d, dash] \\
\bigcap_{n\geq 0} p^n\mathbb{Z}_p = \{0\}
\end{tikzcd}$$

We already know that the topological closure of $\mathbb{Q}$ is $\mathbb{Q}_p$ (because of the definition of completion). One might ask whether something similar happens with the integer numbers and the p-adic integers. The answer is positive as the following theorem shows.

Theorem 6.5.5. *We have $\overline{\mathbb{Z}} = \mathbb{Z}_p$. More precisely, for every $x \in \mathbb{Z}_p$,*

(i) *For all $n \geq 1$ there exists a unique $\alpha_n \in \{0, 1, \dots, p^n - 1\}$ such that $\alpha_n \equiv x \pmod{p^n}$, i.e. $p^n \mid \alpha_n - x$ (or equivalently, $|\alpha_n - x|_p \leq p^{-n}$).*

(ii) *The sequence $\{\alpha_n\}_{n\in\mathbb{N}}$ of* (i) *converges to x.*

Proof. The inclusion $\mathbb{Z}_p \subseteq \overline{\mathbb{Z}}$ will directly follow from (ii), using Lemma 3.1.3. In order to show $\overline{\mathbb{Z}} \subseteq \mathbb{Z}_p$, take $y \in \overline{\mathbb{Z}}$. Again, by Lemma 3.1.3, there exists a sequence $(y_n)_{n\in\mathbb{N}} \subseteq \mathbb{Z}$ converging to y. By the inequality

$$||y_n|_p - |y|_p| \leq |y_n - y|_p$$

it easily follows that

$$\{|y_n|_p\} \to |y|_p.$$

Now, since $y_n \in \mathbb{Z}$ we have $|y_n|_p \leq 1$ for all $n \in \mathbb{N}$. Taking limits, $|y| \leq 1$ and so $y \in \mathbb{Z}_p$, as desired.

Let us prove part (i). For the existence, let $x \in \mathbb{Z}_p$. Since $\mathbb{Z}_p \subseteq \mathbb{Q}_p = \overline{\mathbb{Q}}$, for all $n \in \mathbb{N}$, there exists $\frac{a}{b} \in \mathbb{Q}$ such that

$$\left|x - \frac{a}{b}\right|_p \leq p^{-n}.$$

Instead of the quotient $\frac{a}{b}$ we would like some integer number satisfying the same inequality. Since $x \in \mathbb{Z}_p$, we have $|x|_p \leq 1$. Moreover, $\left|x - \frac{a}{b}\right|_p \leq p^{-n} \leq 1$. Then

$$\left|\frac{a}{b}\right|_p = \left|x - \left(x - \frac{a}{b}\right)\right|_p \leq \max\left\{|x|_p, \left|x - \frac{a}{b}\right|_p\right\} \leq 1$$

so $\frac{a}{b} \in \mathbb{Z}_{(p)}$, that is, $p \nmid b$. Therefore, there exists $c \in \mathbb{Z}$ such that $bc \equiv 1 \pmod{p^n}$. Now, we'll see that $ac \in \mathbb{Z}$ is a good approximation of $\frac{a}{b} \in \mathbb{Q}$ in the sense that it still satisfies the inequality above. We have

$$\left|\frac{a}{b} - ac\right|_p = \left|\frac{ac}{bc} - ac\right|_p = \left|\frac{ac(1-bc)}{bc}\right|_p.$$

Since $p \nmid b, c$, we have $|b|_p = |c|_p = 1$. Hence,

$$\left|\frac{a}{b} - ac\right|_p = |a(1-bc)|_p \leq p^{-n}.$$

Then

$$|x - ac|_p = \left|\left(x - \frac{a}{b}\right) + \left(\frac{a}{b} - ac\right)\right|_p \leq \max\left\{\left|x - \frac{a}{b}\right|_p, \left|\frac{a}{b} - ac\right|_p\right\} \leq p^{-n}.$$

Finally, write $ac = q_n p^n + \alpha_n$ with $0 \leq \alpha_n \leq p^n - 1$. Then

$$|ac - \alpha_n|_p = |q_n|_p |p^n|_p \leq p^{-n},$$

so

$$|x - \alpha_n|_p = |(x - ac) + (ac - \alpha_n)|_p \leq \max\{|x - ac|_p, |ac - \alpha_n|_p\} \leq p^{-n}$$

as we wanted to prove.

For the uniqueness, assume that there exists $\beta_n \in \{0, 1, \ldots, p^n - 1\}$ such that $x \equiv \beta_n \pmod{p^n}$. Then $\alpha_n \equiv \beta_n \pmod{p^n}$ and since $\alpha_n, \beta_n \in \{0, 1 \ldots, p^n - 1\}$, we have that $\alpha_n = \beta_n$.

Part (ii) follows directly from the inequality $|x - \alpha_n|_p \leq p^{-n}$. □

Finally, we have the following important theorem, which provides an alternative a much easier description of the elements in $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

Theorem 6.5.6. *We have*

$$\mathbb{Z}_p = \left\{\sum_{n \geq 0} a_n p^n \mid a_n \in \{0, 1, \ldots, p-1\}\right\}$$

and

$$\mathbb{Q}_p = \left\{\sum_{n \geq -n_0} a_n p^n \mid a_n \in \{0, 1, \ldots, p-1\}, \text{ for some } n_0 \in \mathbb{N}\right\}$$

with no elements repeated in any of them.

Proof. First of all, observe that all the series are really convergent on $\mathbb{Q}_p$. In fact,

$$\sum_{n\geq 0} a_n p^n$$

is Cauchy because

$$\lim_{n\to\infty} a_n p^n = 0$$

and since $\mathbb{Q}_p$ is complete by Proposition 6.4.1, then the series converges. For one inclusion, since

$$\sum_{n\geq 0} a_n p^n = \lim_{n\to\infty} \sum_{k=0}^{n} a_k p^k$$

then

$$\sum_{k=0}^{n} a_k p^k \in \mathbb{Z} \implies \left| \sum_{n\geq 0} a_n p^n \right|_p \leq 1 \implies \sum_{n\geq 0} a_n p^n \in \mathbb{Z}_p.$$

For the opposite inclusion, take $x \in \mathbb{Z}_p$ and consider the sequence $(\alpha_n)_{n\in\mathbb{N}}$ as in Theorem 6.5.5. We have

$$x \equiv \alpha_n \pmod{p^n} \implies x \equiv \alpha_n \pmod{p^{n-1}}$$

and $x \equiv \alpha_{n-1} \pmod{p^{n-1}}$. This implies that $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$. Since $\alpha_{n-1} \in \{0, 1, \ldots, p^{n-1} - 1\}$ and $\alpha_n \in \{0, 1, \ldots, p^n - 1\}$. both are of the form

$$\alpha_{n-1} = \sum_{i=0}^{n-2} a_i p^i \text{ and } \alpha_n = \sum_{i=0}^{n-1} b_i p^i = \sum_{i=0}^{n-2} b_i p^i + b_{n-1} p^{n-1}$$

and since $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$ we have that

$$\sum_{i=0}^{n-2} b_i p^i = \alpha_{n-1}.$$

Therefore,

$$\alpha_n = \alpha_{n-1} + b_{n-1} p^{n-1}.$$

So $(\alpha_n)_{n\in\mathbb{N}}$ is nothing but the partial sums of a series

$$\sum_{n\geq 0} a_n p^n$$

that by Theorem 6.5.5 that series converges to x, i.e.,

$$x = \sum_{n\geq 0} a_n p^n.$$

Now consider an arbitrary $x \in \mathbb{Q}_p$. Then

$$
\begin{aligned}
|x|_p = p^{n_0} \implies \frac{1}{p^{n_0}}|x|_p = 1 \implies |p^{n_0}x|_p = 1 \implies p^{n_0}x \in \mathbb{Z}_p \\
\implies p^{n_0}x = \sum_{n\geq 0} a_n p^n \implies x = \sum_{n\geq 0} a_n p^{n-n_0} = \sum_{n\geq -n_0} a_{n+n_0} p^n.
\end{aligned}
$$

$\square$

Remark. It is well known that

$$
\mathbb{R} = \left\{ \sum_{n\geq -n_0} a_n \left(\frac{1}{10}\right)^n \mid a_n \in \{0, \dots, 9\}, \text{ for some } n_0 \in \mathbb{N} \right\}.
$$

Here, $1 = 0.\widehat{9}$. However when we are dealing with p-adic expansions this, by the previous theorem, is something that can not happen.

Remarks. (1) In the last part of the proof of Theorem 6.5.6. we saw that every $x \in \mathbb{Q}_p$ can be written as

$$
x = \frac{y}{p^{n_0}}
$$

with $y,\ p^{n_0} \in \mathbb{Z}_p$. Then $\mathbb{Q}_p$ is the field of quotients of $\mathbb{Z}_p$.

(2) $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are not countable. Then $\mathbb{Q}$ can not be complete.

(3) A positive integer has a finite p-adic expansion. However, this is not generally true for negative integers. We are going to prove that

$$
-1 = \sum_{n=0}^{\infty} (p-1)p^n.
$$

The series is convergent because $|p|_p < 1$. We can consider the partial sums

$$
\sum_{n=0}^{k} p^n = \frac{1-p^{k+1}}{1-p} \underset{k\to\infty}{\to} \frac{1}{1-p}.
$$

and then we have

$$
\sum_{n=0}^{\infty} (p-1)p^n = (p-1)\sum_{n=0}^{\infty} p^n = (p-1)\frac{1}{1-p} = -1.
$$

Now we are going to see some topological properties of $\mathbb{Q}_p$ and $\mathbb{Z}_p$.

Proposition 6.5.7. *Let p be a prime. Then*

(i) *$\mathbb{Q}_p$ and $\mathbb{Z}_p$ are Hausdorff;*

(ii) *$\mathbb{Q}_p$ and $\mathbb{Z}_p$ are totally disconnected;*

(iii) $\mathbb{Q}_p$ *and* $\mathbb{Z}_p$ *are complete;*

(iv) $\mathbb{Z}_p$ *is compact but* $\mathbb{Q}_p$ *is not compact.*

Proof. Property (i) follows from both being metric spaces and (ii) from being ultrametric spaces according to Problem 16. Regarding (iii), $\mathbb{Q}_p$ is complete by definition and since $\mathbb{Z}_p = \overline{\mathbb{Z}}$, it is closed an it is a subset of $\mathbb{Q}_p$ which is complete so applying Proposition 4.2.1, $\mathbb{Z}_p$ is complete. Let us prove now that $\mathbb{Z}_p$ is compact. According to Theorem 4.2.5 it is enough to see that it is complete and totally bounded. We already know that it is complete so let us show the other condition. Firstly,

$$\overline{B}\left(i, \frac{1}{p^n}\right) = i + p^n\mathbb{Z}_p = B\left(i, \frac{1}{p^{n-1}}\right)$$

are open. Then we can write $\mathbb{Z}_p$ as union of cosets (which form a partition):

$$\mathbb{Z}_p = \bigcup_{i=0}^{p^n-1} \overline{B}\left(i, \frac{1}{p^n}\right) = \bigcup_{i=0}^{p^n-1} B\left(i, \frac{1}{p^{n-1}}\right).$$

Hence, for all $\varepsilon > 0$ there exists $n \in \mathbb{N}$ such that $\frac{1}{p^{n-1}} < \varepsilon$ and so

$$\mathbb{Z}_p = \bigcup_{i=0}^{p^n-1} B\left(i, \frac{1}{p^{n-1}}\right) = \bigcup_{i=0}^{p^n-1} B\left(i, \varepsilon\right),$$

that is,d for all $\varepsilon > 0$, $\mathbb{Z}_p$ can be covered by a finite number of balls, of radius ε, i.e., $\mathbb{Z}_p$ is totally bounded.

Now we are going to see that $\mathbb{Q}_p$ is not compact. According to Theorem 6.5.6,

$$\mathbb{Q}_p = \bigcup_{n\geq 0} \tfrac{1}{p^n}\mathbb{Z}_p$$

is an open infinite cover of $\mathbb{Q}_p$. It does not have finite subcovers. Assume by contradiction that

$$\mathbb{Q}_p = \bigcup_{i=1}^{k} \tfrac{1}{p^{n_i}}\mathbb{Z}_p.$$

Let $n_0 = \max\{n_i \mid i \in \{1, \ldots, k\}\}$. Then we would have $\mathbb{Q}_p = \frac{1}{p^{n_0}}\mathbb{Z}_p$, contradiction.

$\square$

Definition 6.5.8. A topological space is *locally compact* if every point has a compact neighborhood.

Examples 6.5.9. (1) Clearly, $\mathbb{R}$ is not compact but it is locally compact.

(2) $\mathbb{Q}_p$ is not compact but it is locally compact. Let us observe why it is locally compact. Take $x \in \mathbb{Q}_p$. Then $\overline{B}(x, 1)$ is a neighborhood of x and

$$\overline{B}(x, 1) = x + \overline{B}(0, 1) = x + \mathbb{Z}_p$$

Now $x + \mathbb{Z}_p$ is homeomorphic to $\mathbb{Z}_p$, which is compact so the first one is also compact.

6.6 An alternative way to construct $\mathbb{Z}_p$ and $\mathbb{Q}_p$

In this section we present an alternative approach to define the p-adic integers and p-adic numbers, with a more algebraic flavor. We will start constructing the ring $\mathbb{Z}_p$ and then $\mathbb{Q}_p$ will be the field of quotients.

Recall that any $\alpha \in \mathbb{Z}_p$ can be uniquely written as

$$\alpha = \sum_{k \geq 0} a_k p^k$$

with $a_k \in \{0, 1, \ldots p - 1\}$.

For each $n \in \mathbb{N}$, we set

$$\alpha_n = \sum_{k=0}^{n-1} a_k p^k,$$

i.e. the nth partial sum of the series. We already know that $\alpha_n \in \{0, 1, \ldots, p^n - 1\}$.

Hence, with the notation above, we can define the ring-homomorphisms

$$\begin{array}{rccc} \varphi_n \colon & \mathbb{Z}_p & \to & \mathbb{Z}/p^n\mathbb{Z} \\ & \alpha & \mapsto & \varphi_n(\alpha) = \alpha_n + p^n\mathbb{Z}. \end{array}$$

We'll also need the following lemmas about the maps φ_n:

Lemma 6.6.1. *For each $n \in \mathbb{N}$ the homomorphisms φ_n satisfy that*

$$\ker \varphi_n = p^n\mathbb{Z}_p.$$

Proof. We have

$$\begin{aligned} \ker \varphi_n &= \left\{ \alpha = \sum_{k \geq 0} a_k p^k \mid a_k = 0 \text{ for } k = 0, 1, \ldots n - 1 \right\} \\ &= \left\{ \alpha = \sum_{k \geq n} a_k p^k \in \mathbb{Z}_p \right\} = \left\{ \alpha = \sum_{k \geq 0} a_{k+n} p^{k+n} \in \mathbb{Z}_p \right\} = p^n\mathbb{Z}_p. \end{aligned}$$

□

Lemma 6.6.2. *Consider the rings $\mathbb{Z}/p^n\mathbb{Z}$ with the discrete topology and $\mathbb{Z}_p$ with the p-adic topology. Then for all $n \in \mathbb{N}$, the map φ_n is continuous.*

Proof. Let $\alpha = \sum_{k\geq 0} a_k p^k \in \mathbb{Z}_p$ and write $\varphi_n(\alpha) = \alpha_n$. The discrete topology admits a basis of neighborhoods $\{\mathcal{B}_x\}_{x\in\mathbb{Z}/p^n\mathbb{Z}}$ consisting of singletons. Hence, let $B = \{\alpha_n\} \in \mathcal{B}_{\alpha_n}$. Our aim is to show that $\varphi_n^{-1}(B) \in \mathcal{N}_\alpha$.

We have

$$\begin{aligned}
\varphi_n^{-1}(B) = \varphi_n^{-1}(\{\alpha_n\}) &= \left\{ \beta = \sum_{k\geq 0} b_k p^k \in \mathbb{Z}_p \mid \beta_n = \alpha_n \right\} \\
&= \left\{ \alpha_n + \sum_{k\geq n} b_k p^k \in \mathbb{Z}_p \right\} = \alpha_n + \left\{ \sum_{k\geq 0} b_{k+n} p^{k+n} \in \mathbb{Z}_p \right\} \\
&= \alpha_n + p^n\mathbb{Z}_p = \overline{B}\left(\alpha_n, \frac{1}{p^n}\right).
\end{aligned}$$

Since $\varphi_n(\alpha) = \alpha_n$, we have $\alpha \in \varphi_n^{-1}(B) = \overline{B}\left(\alpha_n, \frac{1}{p^n}\right)$ and by Proposition 6.1.13 the closed ball is open, so $\varphi_n^{-1}(B) \in \mathcal{N}_\alpha$. $\square$

Now we introduce another family of mappings. For each $n \in \mathbb{N}$, let

$$\begin{array}{rccc}
\pi_n\colon & \mathbb{Z}/p^n\mathbb{Z} & \to & \mathbb{Z}/p^{n-1}\mathbb{Z} \\
& x + p^n\mathbb{Z} & \mapsto & \pi_n(x + p^n\mathbb{Z}) = x + p^{n-1}\mathbb{Z}.
\end{array}$$

The following diagram shows all the maps that we have defined so far:

$$\begin{tikzcd}
 & & \alpha \in \mathbb{Z}_p \arrow[dl, "\varphi_n"'] \arrow[d, "\varphi_{n-1}"] \arrow[drr, "\varphi_m"] \arrow[drrrr, "\varphi_1"] & & & & \\
\cdots & \mathbb{Z}/p^n\mathbb{Z} \arrow[r, "\pi_n"] & \mathbb{Z}/p^{n-1}\mathbb{Z} \arrow[r, "\pi_{n-1}"] & \cdots \arrow[r, "\pi_{m+1}"] & \mathbb{Z}/p^m\mathbb{Z} \arrow[r, "\pi_m"] & \cdots \arrow[r, "\pi_2"] & \mathbb{Z}/p\mathbb{Z}
\end{tikzcd}$$

There is a natural map from $\mathbb{Z}_p$ into the cartesian product $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$. Indeed, define

$$\begin{array}{rccc}
\varphi\colon & \mathbb{Z}_p & \to & \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \\
& \alpha & \mapsto & \varphi(\alpha) = (\varphi_n(\alpha))_{n\in\mathbb{N}}.
\end{array}$$

We will consider the product $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ with the Tychonoff topology (recall that we take $\mathbb{Z}/p^n\mathbb{Z}$ with the discrete topology). Notice that the product is not the discrete topology because $\mathbb{N}$ is infinite. Moreover, the product is also a ring with the componentwise operations between the sequences.

If φ were an isomorphism between rings and a homeomorphism, then we would have an alternative definition of $\mathbb{Z}_p$ (because $\mathbb{Z}_p$ and $\prod_{n\in\mathbb{N}}\mathbb{Z}/p^n\mathbb{Z}$ would be indistinguishable topologically and algebraically). Nevertheless, the map φ is not onto. It'll turn out that once that φ is restricted to its image, it is a isomorphism and homeomorphism.

In order to prove so, we shall introduce some new concepts which will be useful.

Definition 6.6.3. We say that a sequence $(x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}}\mathbb{Z}/p^n\mathbb{Z}$ is *coherent* if $\pi_n(x_n) = x_{n-1}$ for all $n > 1$.

Definition 6.6.4. The set of all coherent sequences in $\prod_{n\in\mathbb{N}}\mathbb{Z}/p^n\mathbb{Z}$ is said to be the *inverse limit* and it is denoted by $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

Remark. In Chapter 9, we will study some concepts such as inverse systems and inverse limits with more generality, and these definitions will be particular cases of something which is much more general.

Finally, the next theorem is the key for the new definition of $\mathbb{Z}_p$.

Theorem 6.6.5. *The map φ restricted to its image, which is $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, is an isomorphism of topological rings, that is, it is an isomorphism between rings and an homeomorphism.*

Proof. Taking into account that φ_n are homomorphisms between rings for all $n \in \mathbb{N}$, it is clear that so is φ.

Now we see that φ is bijective. On the one hand, according to Lemma 6.6.1, we have that

$$\begin{aligned}\ker\varphi &= \{\alpha \in \mathbb{Z}_p \mid \varphi_n(\alpha) = 0, \forall n \geq 1\}\\ &= \bigcap_{n\in\mathbb{N}} \ker\varphi_n = \bigcap_{n\in\mathbb{N}} p^n\mathbb{Z}_p = \{0\}\end{aligned}$$

and thus φ is injective. On the other hand, to show that it is surjective, we'll check that $\varphi(\mathbb{Z}_p) = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. The inclusion $\varphi(\mathbb{Z}_p) \subseteq \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is clear, so let us prove the opposite one. Let $(x_n)_{n\in\mathbb{N}} \in \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Write $x_n = \alpha_n + p^n\mathbb{Z} = \sum_{k=0}^{n-1} a_{n,k}p^k + p^n\mathbb{Z}$ and

$$x_{n-1} = \alpha_{n-1} + p^{n-1}\mathbb{Z} = \sum_{k=0}^{n-2} a_{n-1,k}p^k + p^{n-1}\mathbb{Z}.$$

Since the sequence is coherent, $a_{n-1,k}$ and $a_{n,k}$ do not depend on n, so write $a_{n-1,k} = a_{n,k} = a_k$. Hence, we have that $\varphi\left(\sum_{k\geq 0} a_k p^k\right) = (x_n)_{n\in\mathbb{N}}$ and φ is surjective.

We have proved that φ is an isomorphism of rings. To see that it is continuous, by the Universal Property of product spaces, it is enough to show that it is continuous in each component, i.e. that for all $n \in \mathbb{N}$, φ_n is continuous. We have already proved that in Lemma 6.6.2, so φ is continuous.

To prove that φ is an homeomorphism, we can show that it is closed as a map. Firstly, notice that $\mathbb{Z}_p$ is compact by Proposition 6.5.7. Moreover, for all $n \in \mathbb{N}$, $\mathbb{Z}/p^n\mathbb{Z}$ is Hausdorff, and so by Problem 1 it follows that $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ is Hausdorff. Hence, the subspace $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is Hausdorff. Now, φ is a continuous map from a compact space into a Hausdorff space, and so it is closed. Thus φ is an isomorphism of topological rings. □

Remark. Now it is clear that $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, the set of coherent sequences, is an alternative way to see the p-adic integers. Indeed, we could have initially defined the p-adic integers using this approach, and then the field of p-adic numbers $\mathbb{Q}_p$, can be seen as the field of quotients of the p-adic integers. However, to do so, we have to be sure that $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is an Integral Domain (ID). In fact, we already know that it is an ID, because in the previous theorem we have proved that it is isomorphic to an ID. Now, think that we have initially defined the p-adic integers as $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ and that we don't know whether it is an ID or not. The next proposition proves that it is an ID, just using the new definition.

Proposition 6.6.6. *The ring $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is an Integral Domain.*

Proof. Let $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ two non-zero coherent sequences. We have to prove that the product is non-zero. For each $n \in \mathbb{N}$ we will write $x_n = \alpha_n + p^n\mathbb{Z}$ and $y_n = \beta_n + p^n\mathbb{Z}$. Since $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \neq 0$, assume that $x_N \neq 0$ and $y_M \neq 0$. If we prove that $x_{2N+2M} \cdot y_{2N+2M} \neq 0$, we have finished.

Assume by way of contradiction that $x_{2N+2M} \cdot y_{2N+2M} = 0$, that is, $p^{2N+2M} \mid \alpha_{2N+2M} \cdot \beta_{2N+2M}$. Then $p^{N+M} \mid \alpha_{2N+2M}$ or $p^{N+M} \mid \beta_{2N+2M}$. Hence, $p^N \mid \alpha_{2N+2M}$ or $p^M \mid \beta_{2N+2M}$. Assume that the first possibility holds, that is, $p^N \mid \alpha_{2N+2M}$ (the one concerning β_{2N+2M} can be done in the same fashion). Then from the coherence condition we have that

$$\begin{aligned} 0 + p^N\mathbb{Z} = \alpha_{2N+2M} + p^N\mathbb{Z} &= \left(\pi_{2N+2M} \circ \overset{N+2M}{\cdots} \circ \pi_{2N+2M}\right)(\alpha_{2N+2M} + p^N\mathbb{Z}) \\ &= \alpha_N + p^N\mathbb{Z}, \end{aligned}$$

and thus $x_N = 0$, which is a contradiction. Hence $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is an ID. □

6.7 Solving polynomial equations over $\mathbb{Z}_p$

Since the ring of p-adic integers is a PID and in particular a UFD, we have available some machinery concerning irreducibility of polynomials in $\mathbb{Z}_p[x]$ and $\mathbb{Q}_p[x]$. General results as Gauss irreducibility criterion or Eisenstein criterion are also valid there, but these results require in practice a good control over the prime elements of the ring we are working, which is not trivial in this case. In this section we will focus our efforts in developing methods find roots of polynomials with coefficients in the concrete ring $\mathbb{Z}_p$. In order to do that we will do something very usual in Algebra, reduce the problem to a better known context.

Consider a polynomial

$$f(x) = \sum_{k=0}^{n} c_k x^k \in \mathbb{Z}_p[x].$$

We know that if A is a UFD, K its field of fractions, $f(x) = \sum_{k=0}^{n} c_k x^k \in A[x]$ and if $\frac{a}{b} \in K$ is a root of f, then $a \mid c_o$ and $b \mid c_n$. Since $\mathbb{Z}_p$ is a UFD this also holds for it.

Considering the map

$$\varphi_n \colon \mathbb{Z}_p[x] \to \mathbb{Z}/p^n\mathbb{Z}[x]$$

such that

$$\varphi_n(f(x)) = \overline{f}(x) = \sum_{k=0}^{n} \overline{c_k} x^k$$

it is also true that if $f(\alpha) = 0$ for $\alpha \in \mathbb{Z}_p$, then $\overline{f}(\overline{\alpha}) = \overline{0}$ in $\mathbb{Z}/p^n\mathbb{Z}$, $\forall n \geq 1$. Now we are going to prove that the converse is also true, but before doing it we need to know a property of compact spaces stated in the following lemma.

Lemma 6.7.1 (Finite intersection property)**.** *Let X be a compact space and let $\{F_i\}_{i\in I} \subseteq X$ be a family of closed sets such that the intersection of finitely many of them is non-empty. Then $\cap_{i\in I} F_i \neq \varnothing$.*

Proof. We argue by contradiction, so suppose we have

$$\bigcap_{i\in I} F_i = \varnothing \implies \bigcup_{i\in I} (X \smallsetminus F_i) = X$$

and since X is compact and $\{X \smallsetminus F_i\}_{i\in I}$ is an open covering of X,

$$X = (X \smallsetminus F_{i_1}) \cup \ldots \cup (X \smallsetminus F_{i_k}))$$

so taking complements

$$\varnothing = F_{i_1} \cap \ldots \cap F_{i_k}$$

that is a contradiction. □

Theorem 6.7.2. *A polynomial $f(x) \in \mathbb{Z}_p[x]$ has a root in $\mathbb{Z}_p$ if and only if it has roots in $\mathbb{Z}/p^n\mathbb{Z}$, $\forall n \geq 1$.*

Proof. As we have previously stated the "only if" is already proved.

Now assume that we have a root $x_n \in \mathbb{Z}/p^n\mathbb{Z}$, for all $n \geq 1$. We want to find α such that $f(\alpha) \equiv 0 \pmod{p^n}$, for all $n \geq 1$ because it implies that $f(\alpha) \in p^n\mathbb{Z}_p$ for all $n \geq 1$ and so $f(\alpha) \in \bigcap_{n\geq 1} p^n\mathbb{Z}_p = \{0\}$.

Let us consider

$$X_n = \{\alpha \in \mathbb{Z}_p \mid f(\alpha) \equiv 0 \pmod{p^n}\}.$$

Then $\ldots \subseteq X_n \subseteq X_{n-1} \subseteq \ldots \subseteq X_1$. By hypothesis, X_n is non-empty for each $n \in \mathbb{N}$. We want to prove that $\bigcap_{n\geq 1} X_n \neq \varnothing$.

We can consider the corresponding polynomial function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$, which is continuous and by Lemma 6.6.2, $\varphi_n\colon \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}_p$ are also continuous for each $n \in \mathbb{N}$. Then the composition $f_n = \varphi_n \circ f\colon \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}_p$ is continuous, so $X_n = f_n^{-1}(0)$ is closed (note that $\{0\}$ is closed because our space is T_1).

Moreover, $X_{n_1} \cap X_{n_2} \cap \ldots \cap X_{n_k} = X_n \neq \varnothing$ for $n = \max\{n_1, \ldots, n_k\}$. Therefore, since $\mathbb{Z}_p$ is compact, applying the previous lemma we have that $\bigcap_{n\geq 1} X_n \neq \varnothing$. □

This result opens the path from the abstruse land of p-adic integers to the well-known that of residue classes of integers, where finding roots is in principle a much more trivial matter. Unfortunately, proving that a polynomial has a root in $\mathbb{Z}/p^n\mathbb{Z}[x]$ for all natural n is not easy, so in practice this theorem does not seem to be very useful. Nevertheless, it will be very helpful to prove the so-called Hensel's lemma, which turns out to be fundamental in theory and practice, because allows us to find roots of polynomials in $\mathbb{Z}_p[x]$ easily.

Theorem 6.7.3 (Hensel's lemma)**.** *Let $f(x) \in \mathbb{Z}_p[x]$ and assume that the reduction modulo p of f has a root α_1 which is a simple root. Then there exists a unique $\alpha \in \mathbb{Z}_p$ which is a root of $f(x)$ and $\alpha \equiv \alpha_1 \pmod{p}$.*

Proof. According to Theorem 6.7.2, we need to produce roots $\alpha_n \in \mathbb{Z}/p^n\mathbb{Z}$, for all $n \geq 1$. We do it by induction on n. For $n = 1$ it is just by the hypothesis, so let us prove it for n. By induction hypothesis there exists $\alpha_{n-1} = x_{n-1} + p^{n-1}\mathbb{Z}$ root of f modulo p^{n-1} and then $p^{n-1} \mid f(x_{n-1})$.

Consider now $x_n = x_{n-1} + p^{n-1}\lambda$ and let us see that $p^n \mid f(x_n)$ for some λ. Then $\alpha_n = x_n + p^n\mathbb{Z}$ will be a root of f modulo p^n.

We know that the Taylor expansion of a polynomial of degree m (in characteristic 0) with respect to a point a is

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2}(x-a)^2 + \frac{f'''(a)}{3!}(x-a)^3 + \cdots + \frac{f^{(m)}(a)}{m!}(x-a)^m$$

and applying it to $f(x_n)$ with respect to the point $a = x_{n-1}$ we have the following

$$\begin{aligned} f(x_n) &= f(x_{n-1}) + f'(x_{n-1})(x_n - x_{n-1}) + \frac{f''(x_{n-1})}{2}(x_n - x_{n-1})^2 + \cdots \\ &= f(x_{n-1}) + f'(x_{n-1})p^{n-1}\lambda + \frac{f''(x_{n-1})}{2}p^{2(n-1)}\lambda^2 + \cdots \end{aligned}$$

and doing it modulo p^n we have

$$f(x_n) \equiv f(x_{n-1}) + f'(x_{n-1})p^{n-1}\lambda = p^{n-1}y_{n-1} + f'(x_{n-1})p^{n-1}\lambda$$

for some $y_{n-1} \in \mathbb{Z}$.

Therefore

$$\begin{aligned} p^n \mid f(x_n) &\iff p \mid y_{n-1} + f'(x_{n-1})\lambda \iff \\ &\iff f'(x_{n-1})\lambda + y_{n-1} \equiv 0 \pmod p \end{aligned}$$

Now since $x_{n-1} \equiv x_1 \pmod p$ and $\alpha_1 = x_1 + p\mathbb{Z}$ is simple then $f'(\alpha_1) \neq \overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$ so $f'(x_1) \not\equiv 0 \pmod p$. Hence,

$$f'(x_{n-1})\lambda + y_{n-1} \equiv 0 \pmod p \iff f'(x_1)\lambda + y_{n-1} \equiv 0 \pmod p$$

and since this is a linear equation in λ over $\mathbb{F}_p$ with non-zero coefficients, it has a unique solution. □

6.7.1 Primitive roots of unity

Any student that delves into the theory of field extensions may find curious how the huge jump from $\mathbb{Q}$ to $\mathbb{R}$ has no effect on the roots of unity. However, when we go from $\mathbb{R}$ to $\mathbb{C}$ (a small step for an algebraist but a giant leap for mankind), we automatically obtain all roots of unity for any natural number, because the field of complex numbers is algebraically closed. In this part, with the invaluable help of Hensel's lemma, we will completely determine which primitive roots of unity are contained in fields of p-adic numbers.

It is immediate that roots of unity in $\mathbb{Q}_p$ are actually contained in the ring of p-adic integers. Indeed, if u is a nth root of unity in $\mathbb{Q}_p$ then we have

$$u^n = 1 \implies |u^n|_p = |u|_p^n = |1|_p = 1 \implies |u|_p = 1 \implies u \in \mathbb{Z}_p.$$

Naturally, u is an invertible element of $\mathbb{Z}_p$, because u^{n-1} is clearly its inverse. The next proposition shows that the situation is not as good as in $\mathbb{C}$.

Proposition 6.7.4. *Let p be a fixed prime and $\mathbb{Q}_p$ the field of p-adic numbers. Then*

(i) *if p is odd, there are not primitive pth roots of unity in $\mathbb{Q}_p$;*

(ii) *if* $p = 2$, *there are not primitive* 4*th roots of unity in* $\mathbb{Q}_p$.

Proof. (i) We shall proof that if $\alpha^p = 1$, then $\alpha = 1$. Projecting the equality to $\mathbb{F}_p$ and taking into account that $\mathbb{F}_p^\times$ has $p-1$ elements we obtain

$$\overline{\alpha^p} = \overline{\alpha}^p = \overline{\alpha} = \overline{1},$$

so $\alpha = 1 + p\lambda$ for some λ contained in $\mathbb{Z}_p$. Of course, our aim now is to show that $\lambda = 0$. By contradiction, suppose that it is not zero. We can write $\lambda = p^{k-1}\mu$ with k natural and p and μ coprime, so $\alpha = 1 + p^k\mu$ and by Newton's binomial we have

$$\alpha^p = (1+p^k\mu)^p = 1 + \binom{p}{1}p^k\mu + \binom{p}{2}p^{2k}\mu^2 + \cdots + p^{pk}\mu^p = 1$$
$$\iff \binom{p}{2}p^{2k}\mu^2 + \cdots + p^{pk}\mu^p = -\binom{p}{1}p^k\mu = -p^{k+1}\mu \neq 0.$$

Given that $p > 2$ we have $pk \geq 2k+1 \geq k+2$, and since p divides $\binom{p}{j}$ for $1 \leq j \leq p-1$ we deduce that p^{k+2} divides the left side of the equality. However, it does not divide the right side, because μ and p are coprime, contradiction.

(ii) By contradiction, assume that α is a primitive 4th root of unity in $\mathbb{Z}_2$. Then it is clear that α^2 is a primitive second root of unity, so it must be -1. Therefore, projecting the equality $\alpha^2 = -1$ to $\mathbb{Z}/4\mathbb{Z}$ we obtain

$$\overline{\alpha}^2 = \overline{-1} = \overline{3}$$

which is clearly impossible (just check the four possible values). □

Remark. Note that in general if ξ is a primitive nth root of unity in an abstract field K and d divides n, then $\xi^{n/d}$ is clearly a primitive dth root of unity. Therefore, the previous proposition also shows that for any natural n there are no primitive pnth roots of unity in $\mathbb{Q}_p$ when p is odd and there are no primitive $4n$th roots of unity in $\mathbb{Q}_2$.

We are now ready to completely determine the primitive roots contained in the fields of p-adic numbers.

Theorem 6.7.5. *Let p be a prime number. We have a primitive mth root of unity contained in $\mathbb{Q}_p$ if and only if*

(i) m *divides* $p-1$ *when* p *is odd or*

(ii) $m = 1, 2$ *when* $p = 2$.

Proof. In order to show the implication $\Leftarrow$) we only have to take care of the odd case, because 1 and -1 are clearly contained in $\mathbb{Q}_2$. The case $m = 1$ is trivial, so we can suppose $m \geq 2$.

It is well known that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, so there exists an element $\overline{\alpha}$ of order m contained there for each divisor of $p-1$. We claim that $\overline{\alpha}$ is a simple root of $f(x) = x^m - \overline{1} \in \mathbb{F}_p[x]$. In effect, the formal derivative of $\overline{f}(x)$ is $\overline{f}'(x) = \overline{m}x^{m-1} \neq \overline{0}$, so the unique root of the formal derivative is $\overline{0}$ and hence $\overline{f}$ has no multiple roots. Therefore, we can apply Hensel's lemma to $f(x) = x^m - 1 \in \mathbb{Z}_p[x]$, which claims that there exists a unique α contained in $\mathbb{Z}_p$ such that $\alpha^m = 1$ and its reduction modulo p is exactly $\overline{\alpha}$. In order to see that it has order m, suppose that $\alpha^k = 1$ for some $k < m$. Reducing modulo p we obtain $\overline{\alpha}^k = \overline{1}$, impossible since $\overline{\alpha}$ has order m.

For the implication $\Rightarrow$) let α be a primitive mth root of unity. Assume first that m and p are coprime. Projecting to $\mathbb{F}_p$ we have that $\overline{\alpha}$ is a root of the polynomial $\overline{f}(x) = x^m - \overline{1}$ in $\mathbb{F}_p$, so $o(\overline{\alpha}) = k$ divides m. Moreover, $\mathbb{F}_p^\times$ is cyclic of order $p-1$, which implies that $o(\overline{\alpha})$ also divides $p-1$. Arguing as before with the formal derivative it can be shown that α is a simple root of $\overline{g}(x) = x^k - \overline{1}$. By Hensel's lemma there exists a *unique* root α^* of $g(x)$ in $\mathbb{Z}_p$ congruent with $\overline{\alpha}$ modulo p. It is clear that α^* is also a root of $f(x)$ in $\mathbb{Z}_p$, so arguing similarly and applying Hensel's lemma to the polynomial $\overline{f}(x)$ with the root $\overline{\alpha}$ we obtain due to the uniqueness the root α^* again. But α is a root of $f(x)$ satisfying

$$\alpha \equiv \overline{\alpha} \equiv \alpha^* \pmod{p},$$

which means that $\alpha = \alpha^*$. Hence, $\alpha^k = 1$ and its order divides $p-1$. Now, if m and p are not coprime it follows that $p \mid m$. By the remark after Proposition 6.7.4 there are no primitive mth roots of unity in $\mathbb{Q}_p$ when p is odd. If $p = 2$, it claims that m cannot be a multiple of 4, so $m = 2m_0$ for some odd natural m_0. In both cases follows the existence of a primitive m_0th root of unity with m_0 and 2 coprime, so according to what we have just proved, m_0 divides $2-1=1$ and $m = 1, 2$, as we wanted to show. □

We will end up showing a rather surprising consequence of this theorem, the existence of an "imaginary unit" in certain fields of p-adic numbers.

Example 6.7.6. According to the previous theorem $\mathbb{Q}_5$ (and in general any $\mathbb{Q}_p$ with $p \equiv 1 \pmod 4$) contains a primitive fourth root of unity, say ξ. Its square is necessarily a primitive second root of unity, so $\xi^2 = -1$, because there are no more.

6.8 Ostrowski's theorem

As seen in Examples 6.1.5 given a UFD R and a prime $p \in R$ we can define the p-adic valuation ν_p in the field of quotients K. Of course, using it we can define a p-adic absolute value $|\ |_p$ in K by

$$\left|\frac{a}{b}\right|_p = c^{\nu_p\left(\frac{a}{b}\right)} = c^{\nu_p(b)-\nu_p(a)},$$

where $a, b \neq 0 \in R$ and c is a fixed real number greater than 1. Note that by Theorem 6.1.17 it does not matter the number c we choose, because we obtain equivalent absolute values. Indeed, if $c, d > 1$ and $|\ |_p$ and $\|\ \|_p$ are defined using those numbers we have

$$\left|\frac{a}{b}\right|_p = c^{\nu_p(b)-\nu_p(a)} = (d^{\nu_p(b)-\nu_p(a)})^{log_d c} = \left\|\frac{a}{b}\right\|_p^{\alpha}$$

for some $\alpha > 0$.

Our aim will be determining all the absolute values that can be defined on $\mathbb{Q}$ and $F(t)$ for certain field F up to equivalence. We will first prove a general result that reduces the amount of work in the concretes cases we are studying. It is worth mentioning that whenever we work with an absolute value on the field of quotients of certain ring R we can prove equivalence just working with elements of R. If $|\ |$ and $\|\ \|$ are equivalent in R we have

$$\|a/b\| = \|a\| \cdot \|b\|^{-1} = |a|^s \cdot (|b|^{-1})^s = |a/b|^s,$$

where $a, b \neq 0 \in R$ and s is certain real number greater than zero.

Lemma 6.8.1. *Let R be a PID and K its field of quotients. Suppose that $|\ |$ is a non-archimedean absolute value on K for which R is included in the ring of integers $\mathcal{O}_K$. Then $|\ |$ is either the trivial absolute value or a p-adic absolute value for some prime $p \in R$.*

Proof. First, let $\mathfrak{m}$ a prime ideal of $\mathcal{O}_K$. We shall see that $\mathfrak{m} \cap R$ is a prime ideal of R. Indeed, it is clearly an ideal of R and if $a, b \in R$ satisfy $ab \in \mathfrak{m} \cap R$ then we have a or b contained in $\mathfrak{m}$ and so in the intersection. In particular, if $\mathfrak{p}$ is the valuation ideal of the absolute value it follows that

$$\mathfrak{a} := \mathfrak{p} \cap R = \{a \in R \mid |a| < 1\}$$

is prime in R.

If $\mathfrak{a} = (0) = \{0\}$ the absolute value of any non-zero element in A is one, so it is clear that in this case we have the trivial absolute value, because for any nonzero element in K we have

$$\left|\frac{a}{b}\right| = |a| \cdot |b|^{-1} = 1 \cdot 1 = 1.$$

Now, suppose that $\mathfrak{a} \neq \{0\}$. Since R is a PID and it is prime, it is generated by some prime element $p \in R$, i.e, $\mathfrak{a} = (p)$. This implies that $|a| < 1$ if and only if $a \in \mathfrak{a}$ if and only if p divides a. In particular, p is the unique prime in R up to associates for which $|p| = r < 1$. Point that the absolute value of the other primes is exactly 1.

A general $a \in R \setminus 0$ can be written in a unique way (except for units) as $a = p^{\nu_p(a)}b$, where $b \in R$, $b \neq 0$ and g.c.d.$(b, p) = 1$. Computing its absolute value we obtain

$$|a| = |p^{\nu_p(a)}b| = |p|^{\nu_p(a)}|b| = |p|^{\nu_p(a)} = r^{\nu_p(a)} = (e^{\nu_p(a)})^{-\log r} = |a|_p^{-\log r}.$$

Since $r < 1$ it follows that $-\log r > 1$. Thus, according to Theorem 6.1.17 $|\ |$ is equivalent to a p-adic absolute value (using in this case the base $c = e$). $\square$

Point that we obtain the trivial absolute value only when $\mathfrak{a} = \{0\}$. If it is not trivial, we obtain a p-adic absolute value.

6.8.1 Ostrowski's theorem in $\mathbb{Q}$.

Theorem 6.8.2. *Every absolute value on $\mathbb{Q}$ is equivalent to:*

(i) *The trivial absolute value, or*

(ii) *The p-adic absolute value for a unique p prime number, or*

(iii) *The usual absolute value, $|\ |_\infty$.*

Proof. According to Theorem 6.1.17 two absolute values are equivalent if there exists a positive real number, α, such that:

$$|x|_1 = |x|_2^\alpha \quad \forall x \in \mathbb{Q}$$

It is enough to prove the firts condition in integer number, instead for all rationals.

Let $\|\ \|$ be a archimedean absolute value. In order to find the desired real number, α, we shall see that the ratio $\|n\|^{\frac{1}{\log n}}$ is constant for all integer numbers.

Take two any integers $m, n > 0$ and write m in the following unique way:

$$m = a_0 + a_1 n + a_2 n^2 + \cdots + a_r n^r \text{ where } 0 \leq a_i < n \text{ and } n^r \leq m$$

Notice, about this two facts:

$$n^r \leq m \implies r \leq \frac{\log m}{\log n} \text{ and } \|a_i\| = \|1+\cdots+1\| \leq \|1\|+\cdots+\|1\| = 1+\cdots+1 \leq n$$

As the absolute value is archimedean $\|n\| \geq 1$ for all integer numbers. Suppose by contradiction that $\|n\| < 1$. Then fixing this number, n, the absolute value of any integer number, m, would be bounded:

$$\|m\| \leq \sum_{i=0}^{r} \|a_i\|\|n\|^i \leq n \sum_{i=0}^{r} \|n\|^i \leq \frac{n}{1 - \|n\|}$$

Ans it is a contradiction because, for a archimedean absolute value, we can find an integer number with an absolute value as large as we want.

Hence, taking the absolute value of m:

$$\|m\| \leq n \sum_{i=0}^{r} \|n\|^i \leq n(1+r)\|n\|^r \leq n \left(1 + \frac{\log m}{\log n}\right) \|n\|^{\frac{\log m}{\log n}}$$

Now, substituting m by m^k and taking the k^{th} root we obtain:

$$\|m\|^k \leq n \left(1 + k\frac{\log m}{\log n}\right) \|n\|^{k\frac{\log m}{\log n}}$$

$$\|m\| \leq \left(n \left(1 + k\frac{\log m}{\log n}\right)\right)^{\frac{1}{k}} \|n\|^{\frac{\log m}{\log n}}$$

By letting $k \to \infty$ we get $\|m\| \leq \|n\|^{\frac{\log m}{\log n}}$, i.e., $\|m\|^{\frac{1}{\log m}} \leq \|n\|^{\frac{1}{\log n}}$, for two any integer numbers. Futhermore, we can interchage m and n in order to obtain the inverse inequality. That is,

$$\|m\|^{\frac{1}{\log m}} = \|n\|^{\frac{1}{\log n}}, \, \forall m, n \in \mathbb{Z}_{>1}$$

Thus the ratio is constant. So for any integer number n choose:

$$\alpha = \log \|n\|^{\frac{1}{\log n}} \implies \|n\| = 10^{\alpha \log n}$$

The choosen is obviously a real number, and its also positive, since both n and $\|n\|$ are values which are greater than one (so their logarithms are positive). Hence, for any $n \neq 0$:

$$\|n\| = \||n|_\infty\| = 10^{\alpha \log |n|_\infty} = |n|_\infty^\alpha$$

Thus, any archimedean absolute value on $\mathbb{Q}$ is equivalent to the usual absolute value: $| \, |_\infty$.

On the other hand, let $\| \, \|$ be a non-archimedean absolute value. According to Lemma 6.8.1 $\| \, \|$ is equivalent either to the trivial absolute value or to a p-adic absolute value for a unique prime number p. $\square$

6.8.2 Ostrowski's Theorem for $F(T)$

Notation. Since there will be only one indeterminate, we will denote f and g the elements of $F[t]$, omitting the variable. Nevertheless, whenever we write t we will refer to that concrete monomial, not to an abstract polynomial.

In the case of fields of rational functions over a field F we have already seen two absolute values: $|f|_\infty = e^{\deg(f)}$ and $|f|_\pi = e^{-\nu_\pi(f)}$, where $\pi \in F[t]$ is an irreducible polynomial and $f = \pi^{\nu_\pi(f)} \cdot f'$ with π and f' coprime. We have only specified the absolute value on the ring of polynomials because its extension to the field of rational functions is completely determined by the properties of absolute values. The Ostrowski's Theorem for $F(t)$ is a little bit more dissapointing that the version for $\mathbb{Q}$, because it classifies all the possible absolutes values on $F(t)$ with an added restriction. Before the theorem, we will need a technical lemma.

Lemma 6.8.3. *Let n be a natural number greater than one, $x_1, \ldots, x_n$ elements of F and $\| \ \|$ an absolute value on F. Then if $|x_n| > |x_i|$ for $i = 1, \ldots, n-1$ we have $|x_1 + \cdots + x_n| = |x_n|$.*

Proof. The case of two elements is a straight consequence of Proposition 6.1.12. Indeed, assume that $|x| > |y| = |-y|$. When $y = 0$ the result is clear, so we can suppose $y \neq 0$. Now consider the triangle whose vertices are 0, x and $-y$. The two longest and equally large sides must be the segments that join 0 and x and $-y$ and x, because the other one is strictly smaller by hypothesis, so $|x| = |x + y|$.
The case of n arbitrary can be reduced to the previous case easily, because if $y = x_1 + \cdots + x_{n-1}$ we have

$$|y| = |x_1 + \cdots + x_{n-1}| \leq \max_{1 \leq i \leq n-1} \{|x_i|\} < |x_n|,$$

so $|(x_1 + \cdots + x_{n-1}) + x_n| = |y + x_n| = |x_n|$, as desired. $\square$

Theorem 6.8.4 (Ostrowski's theorem for $F(t)$)**.** *Every absolute value $\| \ \|$ on $F(t)$ that is trivial on F is either trivial, equivalent to $| \ |_\infty$ or $| \ |_\pi$ for some prime polynomial $\pi \in F[t]$.*

Proof. First, it follows from Theorem 6.1.7 that $\| \ \|$ is nonarchimedean, because it is trivial on F and in particular on the image of $\mathbb{Z}$ in $F(t)$. In order to show the equivalence, we will use again the third characterization of Theorem 6.1.17. Suppose that $f = a_n t^n + \ldots + a_1 t + a_0$ with $a_n \neq 0$. We will distinguish two cases.

Suppose that $\|t\| = c > 1$. Then we have $\|a_i t^i\| = \|a_i\| \cdot \|t\|^i = \|t\|^i < \|t\|^n$ for $i < n$, so according to Lemma 6.8.3 we have

$$\|f\| = \|a_n t^n\| = \|t\|^n = \|t\|^{\deg f} = c^{\deg f} = (e^{\log c})^{\deg f} = |f|_\infty^{\log c}.$$

Since $c > 1$, $\log c > 0$, so $\| \ \|$ is equivalent to $| \ |_\infty$.

Suppose that $\|t\| < 1$. In this case $\|a_i t^i\| = \|t\|^i \leq 1$, so we have $\|f\| \leq 1$, because $\| \ \|$ is nonarchimedean. In particular, this implies that $F[t]$ is included in the valuation ring. Therefore, by Lemma 6.8.1 $\| \ \|$ is trivial or equivalent to $| \ |_\pi$ for certain prime in $F[t]$, as we wanted to show. $\square$

It may seem that we have determined all the possible absolute values on $F(t)$ up to equivalence, but there exist fields of rational functions in which we can define archimedean absolute values. For example, if γ is trascental over $\mathbb{Q}[x]$

we can define for $r(t) \in \mathbb{Q}(t)$ the absolute value $|r(t)|_\gamma = |r(\gamma)|$, where $|\ |$ is in this case the usual absolute value on $\mathbb{R}$. It is in fact an absolute value because $\mathbb{Q}(t)$ is isomorphic to $\mathbb{Q}(\gamma) \subset \mathbb{R}$ in a natural way, so the restriction of the usual absolute value is also an absolute value and it can be translated from one field to the other naturally. However, in case F is finite an absolute value on $F(t)$ must be trivial on F according to Problem 12 (just consider the restriction) and the theorem classifies all possible absolute values up to equivalence.

Chapter 7

An introduction to topological groups

7.1 Main concepts

Definition 7.1.1. A *topological group* is a group, with respect to the operation $\cdot$, and also a topological space, with a topology τ, such that the group binary operation function, μ, and the inverse function, ι,

$$\mu\colon G \times G \to G \text{ such that } \mu(x,y) = xy \text{ and}$$

$$\iota\colon G \to G \text{ such that } \iota(x) = x^{-1}$$

respectively, are continuous (note that $G \times G$ is provided with the product topology).

Then a topological group is at the same time an algebraic structure and a topological structure. Thus, one might operate algebraically and talk about continuous functions at the same time. We will provide some examples in order to clarify the concept.

Example 7.1.2. (i) $\mathbb{R}$ with the addition and the usual topology, $(\mathbb{R}, +, \tau_u)$, is a topological group.

(ii) $\mathbb{Z}_p$ with the addition and the topology induced by the p-adic distance, $(\mathbb{R}, +, \tau_p)$, is a topological group.

Now, we will introduce a new topological property: homogeneity. Put it simply, it means that all points behave in the same way topologically.

Definition 7.1.3. A topological space X is said to be *homogeneous* if for any $x, y \in X$ there is a homeomorphism $h\colon X \to X$ such that $h(x) = y$.

The following proposition shows that any topological group is homogeneous, which is not true for general topological space.

Proposition 7.1.4. *All topological groups are homogeneous.*

Proof. Let G be a topological group where ι is the inverse function and μ the product function. Since the identity map $\mathrm{id}\colon G \to G$ such that $\mathrm{id}(g) = g$ and the constant map $f_x\colon G \to G$ such that $f_x(g) = x$ are continuous, so is the map $\varphi_x\colon G \to G \times G$ such that $\varphi_x(g) = (g, x)$.

Thus, the composition $r_x = \mu \circ \varphi_x$ is continuous, and sends g to gx. Reproducing the argument with the inverse function, which is clearly $r_{x^{-1}}$, it is continuous. Hence, r_x is a homeomorphism for any $x \in G$. In particular, given $x, y \in G$ we have that $r_{x^{-1}y}$ is a homeomorphism such that $r_{x^{-1}y}(x) = xx^{-1}y = y$ and we are done. □

In the proof of the previous proposition an interesting homeomorphism r_x has appeared.

Definition 7.1.5. Let $(G, \cdot, \tau)$ be a topological group and $a \in G$. The homeomorphism (see proof of Proposition 7.1.4) $r_a\colon G \to G$ such that $r_a(b) = ba$ is called *right translation*.

In an analogue way it can be defined the *left translation* for any $a \in G$, which is $l_a\colon G \to G$ such that $l_a(b) = ab$.

Topological groups combine algebraic and topological concepts. The following two propositions are great examples of that fact.

Proposition 7.1.6. *Let G be a topological group and H an open* (topologically) *subgroup* (algebraically). *Then H is closed.*

Proof. Suppose H is open. We have that r_t is a homeomorphism for any $t \in G$, and then $r_t(H) = tH$ is open. Futhermore, the cosets give us a disjoint partition of G, where the equivalence relation is given by:

$$x \sim y \iff xH = yH,$$

and we have:

$$G = \dot{\bigcup_{t \in T \subseteq G}} tH \implies G = H \cup \dot{\bigcup_{t \in T - \{1\}}} tH,$$

where T is a set which contains exactly one representative element of each coset.

Finally, $\bigcup_{t \in T - \{1\}} tH$ is open and $H = G \setminus \bigcup_{t \in T - \{1\}} tH$ is closed, because it is the complementary of an open set. □

If the index of H in G is finite, the previous proof is also true if we exchange the words "open" and "closed":

Proposition 7.1.7. *Let G be a topological group and H a closed subgroup with $|G : H| < \infty$. Then H is open.*

The next proposition is a converse of the previous one:

Proposition 7.1.8. *Let G be a compact topological group and H an open subgroup. Then H has got finite index.*

Proof. Reproducing the previous proposition's proof,

$$G = \bigcup_{t \in T} tH.$$

Then $\{tH \mid t \in T\}$ is a covering of G and G is compact, so there exists a finite subcovering of G. However, all the elements in the covering are disjoint, so all of then must be contained in the subcovering. Therefore, the covering has a finite number of elements, i.e. $|T|$, the number of distinct cosets, is finite. Finally, by definition $|G : H| = |T| < \infty$ and we are done. $\square$

As a straightforward consequence of the previous three results, we obtain the following important property for compact topological groups:

Corollary 7.1.9. *Let G be a compact topological group and H a subgroup of G. Then H is open if and only if H is closed and $|G : H| < \infty$.*

Applying the previous propositions many interesting questions can be discussed.

Example 7.1.10. The topological group $(\mathbb{Z}_p, +, \tau)$ is a compact topological group and the subgroup $p\mathbb{Z}_p$ is an open subgroup. Then the quotient $\mathbb{Z}_p/p\mathbb{Z}_p$ is finite (the meaning of *quotient* will be clarified in the next section). Since, $|\mathbb{Z}_p/p\mathbb{Z}_p| = |\mathbb{Z}_p : p\mathbb{Z}_p|$, it is finite.

Finally, once we define any algebraic or topological structure, the next step is always defining the natural application over that structure. And, this notes will not be an exception.

Definition 7.1.11. Let G_1 and G_2 be topological groups and a function $f\colon G_1 \to G_2$. Then, f is a *homomorphism of topological groups* if it is a homomorphism of groups and it is continuous.

Definition 7.1.12. Let G_1 and G_2 be topological groups and $f_1\colon G_1 \to G_2$ a homomorphism of topological groups. We will say that f_1 is an *isomorphism of topological groups* if there exists another homomorphism of topological groups $f_2\colon G_2 \to G_1$ such that $f_1 \circ f_2 = f_2 \circ f_1 = \mathrm{id}$.

The reader can appreciate that an isomorphism of topological groups is a function which at the same time is an isomorphism of groups and a homeomorphism of topological spaces.

Examples 7.1.13. (i) The identity map $\mathrm{id}\colon (\mathbb{R}, +, \tau_{dis}) \to (\mathbb{R}, +, \tau_u)$ is a homomorphism of topological groups. Indeed, the identity is clearly a group homomorphism and it is continuous. However, is not an isomorphism of topological groups, since its inverse, $\mathrm{id}\colon (\mathbb{R}, +, \tau_u) \to (\mathbb{R}, +, \tau_{dis})$, is not continuous.

(ii) Reproducing the previous arguments, the maps $\mathrm{id}\colon (\mathbb{R}, +, \tau_u) \to (\mathbb{R}, +, \tau_{ind})$ and $\mathrm{id}\colon (\mathbb{R}, +, \tau_{dis}) \to (\mathbb{R}, +, \tau_{ind})$ are homomorphisms of topological groups, but they are not isomorphisms of topological groups.

7.2 Separability

In topological spaces studying separability properties is very important. Working with topological groups their analisis is much easier. In fact, the next two results show the relation between those properties.

Theorem 7.2.1. *Let $(G, \cdot, \tau)$ be a topological group. Then the separability properties T_0, T_1 and T_2 are equivalent.*

Proof. For any topological space this implication chain holds:

$$T_2 \Rightarrow T_1 \Rightarrow T_0.$$

Hence, in order to prove the circle of implications we shall show that property T_0 implies property T_1 and that being T_1 implies being T_2.

$T_0 \Rightarrow T_1$. Suppose G is a T_0 topological group. First we prove the implication for the case in which one of the elements is the identity. Take 1 and $z \in G$ and let U be an open subset such that $1 \in U$ and $z \notin U$.

The inverse function is a homeomorphism; so $U' = U \cap \iota(U)$ is an open subset, since is the finite intersection of open sets. And $1 \in U'$, because $1 \in U$ and $1 = \iota(1) \in \iota(U)$. Futhermore, using that the left translation is a homeomorphism, $l_z(U') = zU'$ is an open subset such that $z \in zU'$ and $1 \notin U'$.

Suppose by contradiction that $1 \in zU'$, then:

$$1 = zz^{-1} \in zU' \implies z^{-1} \in \iota(U) \implies \iota(z) \in \iota(U) \implies z \in U,$$

which is a contradiction. Therefore, there exist two open subsets U' and zU', such that: $1 \in U'$, $z \notin U'$, $z \in zU'$ and $1 \notin zU'$.

Now take two points $x \neq y \in G$ and let U be an open subset such that $x \in U$ and $y \notin U$. Then using the case which we have just proved, there exist two open subsets V_1 and V_2 separating the points 1 and $l_{x^{-1}}(y) = x^{-1}y$. Hence, $l_x(V_1) = xV_1$ and $l_x(V_2) = xV_2$ are two open subsets separating x and y, because

$$1 \in V_1 \implies x \in xV_1 \quad \text{and} \quad x^{-1}y \notin V_1 \implies y \notin xV_1$$

$$x^{-1}y \in V_2 \implies y \in xV_2 \quad \text{and} \quad 1 \notin V_2 \implies x \notin xV_2.$$

Therefore, G is T_1.

$T_1 \Rightarrow T_2$. Define the function $\varphi\colon G \times G \to G$ such that $\varphi(a,b) = a^{-1}b$. Notice that $\varphi = \mu \circ \psi$, where, μ is the product map, which is continuous in G, and $\psi\colon G\times G \to G\times G$ such that $\psi(a,b) = (a^{-1}, b)$ (it is continuous because the inverse function is continuous in G, so it is componentwise continuous). Thus, φ is continuous because it is the composition of continuous maps.

Furthermore,

$$\begin{aligned}\varphi^{-1}(\{1\}) &= \ker\varphi \\ &= \{(x,y) \in G \times G \mid \varphi(x,y) = x^{-1}y = 1\} \\ &= \{(x,y) \in G \times G \mid x = y\} = \Delta(G).\end{aligned}$$

Finally, in a T_1 topological space the point $\{1\}$ is closed, so its preimage by a continuous function is also closed, i.e., the diagonal $\Delta(G)$ is closed. Therefore, according to Problem 17, the topological space G is T_2. □

Proposition 7.2.2. *Topological groups are regular.*

Proof. Let G be a topological group. Firstly, we shall see that the identity 1 and a closed set C such that $1 \notin C$, can be separated by two disjoint open subsets.

Since C is closed and does not contain 1, $G \setminus C$ is a open set which contains 1. Then there exists an open neighborhood of the identity, say V, such that

$$V^{-1}V \subseteq G \setminus C \iff x^{-1}y \notin C, \forall x, y \in V \iff y \notin xC, \forall x, y \in V$$

and the last expression holds if and only if $V \cap VC = \varnothing$. Moreover, $VC = \bigcup_{c\in C} r_c(V) = \bigcup_{c\in C} Vc$ is a union of open sets, so it is open. Therefore, we have two open subsets V and VC such that: $1 \in V$, $C \subseteq VC$ and $VC \cap V = \varnothing$. Thus, V and VC separate 1 and C.

Secondly, let F be a closed set such that $x \notin F$. It follows that $x^{-1}F$ is a closed set not containing 1. According to the first part, there exist two open subsets U' and V' separating 1 and $x^{-1}(F)$, respectively. Hence, xU' and xV' are two open subsets separating x and F, respectively. □

Moreover, as a consequence of the previous proposition, we have that in any topological group separability properties T_0, T_1, T_2 and T_3 are equivalent. Nevertheless, in general topological groups are not normal.

7.3 Connected components

Proposition 7.3.1. *Let G be a topological group, then the connected component of G at the identity is a normal subgroup of G.*

Proof. Denote by $C(1)$ the connected component at the identity. First, we shall see that $C(1)$ is a subgroup of G. For any $z \in C(1)$, we have that $r_{z^{-1}}$ is a homeomorphism, so $C(1)$ and $z^{-1}C(1)$ are homeomorphic. In particular, $z^{-1}C(1)$ is connected and $1 = z^{-1}z \in z^{-1}C(1)$. Then by the definition of connected component $z^{-1}C(1) \subseteq C(1)$ so $C(1)$ is a subgroup of G.

Second, we shall see that $C(1)$ is normal. For any $x \in G$, $t_x = c_{x^{-1}} \circ l_x \colon G \to G$ such that $c_x(y) = xyx^{-1}$, it is a homeomorphism. Then $C(1)$ and $xC(1)x^{-1}$ are homeomorphic, and in particular $xC(1)x^{-1}$ is connected and $1 = x1x^{-1} \in xC(1)x^{-1}$. By definition of connected component $xC(1)x^{-1} \subseteq C(1)$, so $C(1)$ is normal. □

Corollary 7.3.2. *Let G be a topological group and $C(1)$ the connected component of G at the identity. Then the quotient (see next section) $G/C(1)$ is totally disconnected.*

7.4 Quotients and isomorphism theorems

Let G be a topological group and choose any subgroup H of G. Consider the equivalence relation given by

$$x \sim y \iff xH = yH.$$

Since G is a topological space and $\sim$ is an equivalence relation, we can always construct the quotient set equipped with the quotient topology. At this point, the following notation will be more convenient.

Notation. In the case of the equivalence relation $\sim$ defined above, the quotient set $G/\sim$ will be denoted G/H.

Moreover, the elements of the quotient, i.e. the equivalence classes, are no more than the left-cosets, that is, we have $[x] = xH$ for all $x \in G$.

Recall also that we have the projection map $p \colon G \to G/H$, which is continuous. In general, it is not true that p is open as a map. However, in the case of topological groups, it is open:

Proposition 7.4.1. *Let G be a topological group and H any subgroup. Then the canonical projection $p \colon G \to G/H$ is an open map.*

Proof. Let U be open in G. We have to check that $p(U)$ is open with the quotient topology, i.e., that $p^{-1}(p(U))$ is open. We have that

$$p^{-1}(p(U)) = p^{-1}(\{xH \mid x \in U\}) = \{y \in G \mid xH = yH \text{ for some } x \in U\}.$$

Since cosets form a partition, we have that $xH = yH$ if and only if $y \in xH$ and then, the expression above can be written as

$$p^{-1}(p(U)) = \bigcup_{x \in U} \{y \in G \mid y \in xH\} = \bigcup_{x \in U} xH = UH = \bigcup_{x \in H} Ux.$$

Finally, all Ux are open because they are images of the open set U under the homeomorphisms r_x, and so the union is open.

□

Until now, we have not given any group structure to the quotient. If we want to construct a quotient group, we shall additionally require H to be a normal subgroup. So let us assume that $N \trianglelefteq G$ is a normal subgroup. Then we can see G/N as a topological space (defined as above) and a quotient group. Thus a natural question arises: is the quotient G/N a topological group? The answer is positive as Proposition 7.4.3 shows.

First, we need to recall a lemma from Topology.

Lemma 7.4.2. *Let X, Y and Z be three topological spaces and take $q\colon X \to Y$ a quotient map. Then any map $f\colon Y \to Z$ is continuous if and only if $f \circ q\colon X \to Z$ is continuous.*

$$\begin{tikzcd} X \arrow[d, "q"'] \arrow[dr, "f\circ q"] & \\ Y \arrow[r, "f"'] & Z \end{tikzcd}$$

Proposition 7.4.3. *Let G be a topological group and $N \trianglelefteq G$. Then G/N is a topological group.*

Proof. We have to see that the product and inverse mappings, respectively $\bar{\mu}\colon G/N \times G/N \to G/N$ and $\bar{\iota}\colon G/N \to G/N$, are continuous. Assume that μ and ι are the product and inversion maps defined on G,

$$\begin{tikzcd} G \arrow[r, "\iota"] \arrow[d, "p"'] & G \arrow[d, "p"] \\ G/N \arrow[r, "\bar{\iota}"'] & G/N \end{tikzcd}$$

Lemma 7.4.2 is telling us that $\bar{\iota}$ is continuous if and only if $\bar{\iota} \circ p$ is continuous. Moreover, $\bar{\iota} \circ p = p \circ \iota$ is continuous because it is the composition of continuous applications, so the result follows.

Now, consider the map $p \times p\colon G \times G \to G/N \times G/N$ such that $(p \times p)(a, b) = (aN, bN)$. If we prove that $p \times p$ is a quotient map, we have finished (because the same argument as for ι will prove the continuity). We will see that $p \times p$ is continuous, open and surjective. It is continuous because it is continuous in each component. It is also clear that it is surjective (because so is p). Finally let us prove that the map is open. Take $U \times V \in \beta_{Tych}$ (that is, U and V are open in G). Of course, we have $(p \times p)(U \times V) = p(U) \times p(V)$. Using Proposition 7.4.1, we obtain that $p(U)$ and $p(V)$ are open and so $(p \times p)(U \times V) = p(U) \times p(V)$ is open in the product $G/N \times G/N$.

□

Now we will give versions of the isomorphism theorems for topological groups.

Theorem 7.4.4 (First Isomorphism Theorem)**.** *Let G and H be topological groups and $f\colon G \to H$ be an open, surjective homomorphism of topological groups (that is, continuous and homomorphism of groups). Then the map*

$$\begin{aligned} \varphi\colon G/\ker f &\to H \\ x(\ker f) &\mapsto f(x) \end{aligned}$$

is an isomorphism of topological groups (i.e. an isomorphism of groups and homeomorphism).

Proof. See Problem 18. ☐

Theorem 7.4.5 (Third Isomorphism Theorem)**.** *Let $N \trianglelefteq G$ and $M \trianglelefteq G$ with $N \leq M$. Then we have the following isomorphism of topological groups:*

$$\frac{G/N}{M/N} \cong \frac{G}{M}.$$

Proof. We give a proof in Problem 19. ☐

Nevertheless, the Second isomorphism Theorem fails in topological groups. We have the following counterexample:

Example 7.4.6. Consider the additive group $(\mathbb{R}, +)$ with the usual topology and the normal ($\mathbb{R}$ is abelian group with respect the addition) subgroups $N = \mathbb{Z}$ and $H = \sqrt{2}\mathbb{Z} = \{\sqrt{2}n \mid n \in \mathbb{Z}\}$.

Clearly $H \cap N = \{0\}$, and so $\frac{H}{H \cap N} \cong H = \sqrt{2}\mathbb{Z}$ as topological groups. In particular, both are discrete. However, $H + N = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ is a dense subset of $\mathbb{Z}$, hence $\frac{N+H}{N} = \frac{\mathbb{Z}+\sqrt{2}\mathbb{Z}}{\mathbb{Z}}$ is a *dense* subset of the compact group $\frac{\mathbb{R}}{\mathbb{Z}} \cong \mathbb{S}^1$. In particular, $\frac{\mathbb{Z}+\sqrt{2}\mathbb{Z}}{\mathbb{Z}}$ is not discrete. Thus, $\frac{N+H}{N} \ncong \frac{H}{H \cap N}$ as topological groups.

7.5 Neighborhood bases

One remarkable aspect in topology is the wide range of methods that we have available to construct topological spaces. If we fulfil some conditions, we can create and use subbases, neighborhood systems or even local bases to build topologies that are coherent with the structures we have used. We shall see that the method of the local bases has its analogue in the case of topological groups, with the added perk that we only need to obtain a local base for the identity. This is a really satisfactory fact, because topological groups are quite strong and rich structures, so in general it is difficult to construct them choosing groups and adding topologies ramdomly (and viceversa). As in topology, we start introducing some properties that a local base of the identity always has and then we state and proof the converse, which gives us the mentioned way to obtain topologies over groups. But before it is convenient to introduce a pretty intuitive lemma that claims that once we know a local base of the identity we are in position of obtaining a base of neighborhoods for any other point.

Lemma 7.5.1. *Let $(G, \cdot, \tau)$ be a topological group, $\mathcal{B}$ a local base of the identity and B an element of $\mathcal{B}$. Then for all $x \in G$ the set xB is a neighborhood of the point x and $x\mathcal{B} = \{xB \in \mathcal{P}(G) \mid B \in \mathcal{B}\}$ is a local base of x. The same happens with Bx and $\mathcal{B}x$.*

Proof. Everything follows from l_x being a homeomorphism and $xB = l_x(B)$, because homeomorphisms transform neighborhoods and bases of a point in neighborhoods and bases of its image point. For the other part the argument is the same using r_x. □

Proposition 7.5.2. *Let $(G, \cdot, \tau)$ be a topological group and $\mathcal{B}$ a local base of the identity. Then the following properties hold:*

- $\mathcal{B}_0$) *The identity is contained in every $U \in \mathcal{B}$;*
- $\mathcal{B}_1$) *for each $U, V \in \mathcal{B}$ there exists $W \in \mathcal{B}$ such that $W \subset U \cap V$;*
- $\mathcal{B}_2$) *for each $U \in \mathcal{B}$ there exists $V \in \mathcal{B}$ such that $V \cdot V \subset U$;*
- $\mathcal{B}_3$) *for each $U \in \mathcal{B}$ there exists $V \in \mathcal{B}$ such that $V^{-1} \subset U$ (or equivalently, $V \subset U^{-1}$);*
- $\mathcal{B}_4$) *for each $U \in \mathcal{B}$ and $x \in G$ there exists $V \in \mathcal{B}$ such that $x^{-1}Vx \subset U$ (or equivalently, $Vx \subset xU$).*

Proof. The properties $\mathcal{B}_0$ and $\mathcal{B}_1$ hold in any topological space, because the intersection of neighborhoods is again a neighborhood and they all must contain the identity. Let μ and ι be the product function and the inversion respectively.

For $\mathcal{B}_2$, given $U \in \mathcal{B}$ consider the set $\mu^{-1}(U)$, which is an open neighborhood of $(1, 1)$ due to continuity of μ. Therefore, there exist $V_1, V_2 \in \mathcal{B}$ such that $V_1 \times V_2$ is included in $\mu^{-1}(U)$. Using $\mathcal{B}_1$ we can choose $V \in \mathcal{B}$ included in $V_1 \cap V_2$, and so $V \times V \subset \mu^{-1}(U)$. Therefore, taking into account that μ is surjective and applying it we obtain

$$\mu(V \times V) = V \cdot V \subset \mu(\mu^{-1}(U)) = U,$$

as desired.

Now, consider $V \in B$ included in $\iota^{-1}(U)$, that is a neighborhood of the identity due to continuity of the inversion. Since ι is clearly bijective we have

$$\iota(V) = V^{-1} \subset \iota(\iota^{-1}(U)) = U,$$

which proves $\mathcal{B}_3$.

Finally, the property $\mathcal{B}_4$ is a straight consequence of Lemma 7.5.1, because if x is an element of G and $U \in \mathcal{B}$ then xU is a neighborhood of the point x. But we also know that $\mathcal{B}x$ is a local base of x, so there exists $Vx \in \mathcal{B}x$ (with $V \in \mathcal{B}$) included in xU, as wanted. □

Although $\mathcal{B}_0$ may seem trivial, it is really necessary to avoid problems that appear if we do not control the empty set, because when it is contained in $\mathcal{B}$ all the other properties are trivially satisfied. Actually, it would be enough to require nonemptiness instead of containing the identity, but in practice the gain is not remarkable.

Theorem 7.5.3. *Let $(G, \cdot)$ be a group and $\mathcal{B}$ a nonempty family of subsets of G satisfying the properties $\mathcal{B}_i$ for $i = 0, 1, 2, 3, 4$ of the previous proposition. Then*

$$\tau = \{U \subset G \mid \forall x \in U \ \exists B \in \mathcal{B} \text{ such that } xB \subset U\}$$

is the unique topology satisfying that $(G, \cdot, \tau)$ is a topological group and $\mathcal{B}$ is a local base of the identity.

Proof. The first thing we must show is that τ is really a topology. It is clear that G and the empty set are contained in τ. Let $U_1, U_2 \in \tau$ not disjoint and take $x \in U_1 \cap U_2$. By definition of τ we can choose $B_1, B_2 \in \mathcal{B}$ such that $xB_1 \in U_1$ and $xB_2 \subset U_2$. By $\mathcal{B}_1$ there exists $B_3 \in \mathcal{B}$ such that $B_3 \subset B_1 \cap B_2$, so

$$xB_3 \subset x(B_1 \cap B_2) = xB_1 \cap xB_2 \subset U_1 \cap U_2$$

and τ is closed for intersection. Finally, let $U_i \in \tau$ for $i \in I$. We can suppose that at least one is nonempty and choose $x \in \bigcup_{i \in I} U_i$. Then exists $i_x \in I$ such that $x \in U_{i_x}$ and we can find $B \in \mathcal{B}$ such that $xB \subset U_{i_x} \subset \bigcup_{i \in I} U_i$, so the union is clearly in τ. It is clear by the definition and $\mathcal{B}_0$ that for this topology $\mathcal{B}$ is a open local base of the identity. Furthermore, the definition of the topology also ensures that $x\mathcal{B}$ is a local base of x for any $x \in G$ (note that using $\mathcal{B}_4$ it can be proved that $\mathcal{B}x$ also, but we will not need it).

Now we will prove that the product map μ is continuous with this topology. In order to see that we will show that the preimages of basic neighborhoods are neighborhoods of the corresponding points in each space, using as local base of x in G the set $x\mathcal{B}$. Let $U \in \mathcal{B}$ and consider the neighborhood xyU of xy. We must show that $\mu^{-1}(xyU)$ is a neighborhood of (x, y) in $(G \times G, \tau_{Tych})$. By $\mathcal{B}_2$ there exists V contained in $\mathcal{B}$ such that $V \cdot V \subset B$, and by $\mathcal{B}_4$ there exists $V' \in \mathcal{B}$ such that $V'y \subset yV$. Therefore, $xV' \times yV$ is a neighborhood of (x, y) in $G \times G$ and we have

$$\mu(xV' \times yV) = xV'yV \subset xyVV \subset xyU.$$

Finally, taking preimages we conclude that

$$xV' \times yV \subset \mu^{-1}(\mu(xV' \times yV)) \subset \mu^{-1}(xyU)$$

and $\mu^{-1}(xyU)$ is a neighborhood of (x, y), because it contains another neighborhood of that point.

In order to show that the invertion map ι is continuous, let U be in $\mathcal{B}$ and consider the set $x^{-1}U \in x^{-1}\mathcal{B}$. We have to show that $\iota^{-1}(x^{-1}U) = xU^{-1}$ is a neighborhood of x. By $\mathcal{B}_3$ there exists $V \in \mathcal{B}$ such that $V \subset U^{-1}$, so it follows that xV is included in xU^{-1}, so this set is also a neighborhood of x and therefore ι is continuous.

To finish, we must show the uniqueness of the topology under those conditions. Suppose that τ' is another topology on $(G, \cdot)$ satisfying that $\mathcal{B}$ is a local base of the identity. Then according to Lemma 7.5.1 for each $x \in G$ we can also choose as local base $x\mathcal{B}$, so both topologies admit $\{x\mathcal{B}\}_{x\in G}$ as fundamental system of neighborhoods, which implies that they must be equal. □

We end this section introducing some examples that ilustrate the strength of the result we have proved.

Examples 7.5.4. (1) In $(\mathbb{R}, +)$ the collection $\mathcal{B} = \{(-\epsilon, \epsilon) \subset \mathbb{R} \mid \epsilon > 0\}$ satisfies clearly the conditions of Theorem 7.5.3 and gives us the usual topology.

(2) In $(\mathbb{Z}, +)$ fix a prime p and consider the family $\mathcal{B} = \{p^n\mathbb{Z} \subset \mathbb{Z} \mid n \in \mathbb{N}\}$. Of course, it has all the required properties, because it is a decreasing collection of ideals, which are in particular subgroups of the additive group of the ring $\mathbb{Z}$. Therefore, they all contain the identity, the intersection of two of them is the smallest one, they are closed for the product and inversion and conjugation has nothing to do, because the operation is commutative. It turns out that we obtain in this way the p-adic topology.

(3) Let G be an arbitrary group and consider $\mathcal{B} = \{N \trianglelefteq G \mid |G : N| < \infty\}$. All the properties except $\mathcal{B}_1$ are immediate from the fact that we are again dealing with subgroups (for $\mathcal{B}_4$ we use normality). In order to prove $\mathcal{B}_1$ recall that the intersection of normal subgroups is also normal, so it is enough to show that for any $N_1, N_2 \in \mathcal{B}$ then $N_1 \cap N_2$ has also finite index. It is a consequence of the Second Isomorphism Theorem:

$$\frac{N_1}{N_1 \cap N_2} \cong \frac{N_1 N_2}{N_2} \leq \frac{G}{N_2}$$

so

$$\begin{aligned} |G : N_1 \cap N_2| = |G : N_1||N_1 : N_1 \cap N_2| = \\ = |G : N_1||N_1N_2 : N_2| \leq |G : N_1||G : N_2| < \infty, \end{aligned}$$

as desired. The same argument would be valid if $\mathcal{B}$ were a nonempty family of normal subgroups closed for intersection. Point that the previous example is a particular case of this.

(4) Similarly, it can be shown that the family $\mathcal{B} = \{H \leq G \mid |G : H| < \infty\}$ also satisfies $\mathcal{B}_i$ for $i = 0, \ldots, 4$ and so generates a topology, namely *profinite topology*. Of course, in abelian groups every subgroup is normal and we would be in the previous case, so this is really interesting when G is not abelian.

7.6 Pseudometrizability of topological groups

If we look back and see the path we have already walked, it seems clear, in the words of 1066 and All That, that metric spaces are a Good Thing[1]. Unfortunately, convenient means restrictive almost always, and this case is not an exception, because we have also seen how difficult is having or determining metrizability. Nevertheless, there exists the weaker concept of pseudometric, i.e., a map that fulfils the definition of distance except for the fact that the (pseudo)distance of two different points may be zero, which gives birth to pseudometric spaces. The contruction of a topology from a pseudodistance follows exactly the same idea used with distances, and the same strategy used in that case is valid to show that pseudometrizable spaces are C_I. The aim of this section is showing the converse, first-countable topological groups are also pseudometrizable. We need a pair of lemmas, but we will not prove the one concerning elementary calculus.

Lemma 7.6.1. *Let A and B be subsets of $\mathbb{R}$ and consider the set $A + B = \{a + b \in \mathbb{R} \mid a \in A, b \in B\}$. Then*

(i) *if A is included in B, $\inf A \geq \inf B$;*

(ii) $\inf(A + B) = \inf A + \inf B$.

Lemma 7.6.2. *Let G be a first-countable topological group. Then there exists $\{B_n\}_{n\in\mathbb{N}}$ a decreasing local base of the identity such that for all $n \in N$ we have*

(i) $B_n = B_n^{-1}$ *(B_n is* symmetric*);*

(ii) $B_{n+1}B_{n+1}B_{n+1}$ *is included in B_n.*

Proof. Let $\mathcal{B}$ be a decreasing countable local base of the identity. In case $\mathcal{B}$ is finite of n elements it is clear that $\{B_n\}$ is also a local base that satisfies trivially (i) and (ii), so we can assume that $\mathcal{B}$ is infinite.

For (i) we only have to choose $B'_n = B_n \cap B_n^{-1}$, which is also a neighborhood of the identity due to $\mathcal{B}_1$ and $\mathcal{B}_2$ of Proposition 7.5.2. Point that the base $\mathcal{B}' = \{B'_n \subset G \mid B_n \in \mathcal{B}\}$ is also decreasing.

In order to show (ii) we will use that any infinite subset $\{B_{i_1}, B_{i_2}, \ldots\}$ of $\mathcal{B}$ is also a local base, because i_k can be arbitrarily large and the neighborhoods are

[1]See John M. Howie, *Fields ang Galois Theory*, Springer, 2006, page 106.

decreasing. We will recursively contruct a new local base satisfying (ii). Choose $B_{i_1} = B_1$. By Proposition 7.5.2 we can find $j > i_1$ for which $B_j B_j \subset B_{i_1}$, and similarly $i_2 > j$ for which $B_{i_2} B_{i_2} \subset B_j$, so

$$B_{i_2} B_{i_2} B_{i_2} \subset B_{i_2} B_j \subset B_j B_j \subset B_{i_1}.$$

With the same argument we can find $i_3 > i_2$ for which $B_{i_3} B_{i_3} B_{i_3} \subset B_{i_2}$ and repeating the process idefinitely we can obtain a local base $\{B_{i_k}\}_{k\in\mathbb{N}}$ satisfying (ii) by construction. Point that the new local base is included in $\mathcal{B}$ so the symmetry is preserved in the process. □

Since we are dealing with neighborhoods of the identity, it is clear that $B_i B_j$ includes both neighborhoods. In particular, $B_{n+1}B_{n+1} \subset B_{n+1}B_{n+1}B_{n+1}$, so a local base in the conditions of Lemma 7.6.2 also satisfies that $B_{n+1}B_{n+1} \subset B_n$.

Theorem 7.6.3. *Let $(G, \cdot, \tau)$ be a first-countable topological group. Then it is pseudometrizable.*

Proof. Let $\mathcal{B} = \{B_n \subset G \mid n \in \mathbb{N}\}$ be a decreasing neighborhood base of the identity satisfying the properties of Lemma 7.6.2. We can suppose that $B_1 = G$, just including it in the base and renaming the other ones $B'_{n+1} = B_n$, because the properties of the lemma are clearly preserved. Define $f\colon G \times G \to [0, 1]$ by

$$f(x, y) = \begin{cases} 0 & \text{if } x^{-1}y \in \bigcap\limits_{n\in\mathbb{N}} B_n \\ 2^{-n} & \text{if } x^{-1}y \in B_n \setminus B_{n+1}. \end{cases}$$

It is well defined because there is always a B_i containing the element $x^{-1}y$ (that is the reason why we have included $B_1 = G$) and they are decreasing, so it makes sense to use the greatest natural number for which $x^{-1}y \in B_n$ if such number exists and if not, just assign the value zero. Due to the symmetry of the sets B_i we have that $x^{-1}y \in B_n \setminus B_{n+1}$ if and only if $y^{-1}x \in B_n \setminus B_{n+1}$ (and so happens with the infinite intersection), so for all $x, y \in G$ it follows that $f(x, y) = f(y, x)$. Point that due to $\mathcal{B}_0$ we have $f(x, x) = 0$. Consider the set

$$\begin{aligned} \mathcal{F}_{x,y} &= \{f(x_1, x_2) + \cdots + f(x_k, x_{k+1}) \mid k \in \mathbb{N}, x_i \in G, x_1 = x, x_{k+1} = y\} \\ &= \{f(x_{k+1}, x_k) + \cdots + f(x_2, x_1) \mid k \in \mathbb{N}, x_i \in G, x_1 = x, x_{k+1} = y\} \\ &= \{f(x'_1, x'_2) + \cdots + f(x'_k, x'_{k+1}) \mid k \in \mathbb{N}, x'_i \in G, x'_1 = y, x'_{k+1} = x\} = \mathcal{F}_{y,x} \end{aligned}$$

and define the map $d\colon G \times G \to [0, 1]$ by $d(x, y) = \inf \mathcal{F}_{x,y}$. It is clear that $d \le f$, because $f(x, y) \in \mathcal{F}_{x,y}$. Our purpose will be showing that d is a pseudometric that generates τ.

Since $f \ge 0$ it is clear that $d(x, y) \ge 0$ and $d(x, x) = 0$ follows immediately from $f(x, x) = 0$. Moreover, since $\mathcal{F}_{x,y} = \mathcal{F}_{y,x}$ it follows that d is symmetric. Finally, in the notation of Lemma 7.6.1 we have that $\mathcal{F}_{x,y} + \mathcal{F}_{y,z}$ is included in $\mathcal{F}_{x,z}$ (the sums of the first set necessarily start with $d(x, x_2)$ and end with $d(x_k, y)$ for some natural k), so we have

$$d(x, z) = \inf \mathcal{F}_{x,z} \le \inf(\mathcal{F}_{x,y} + \mathcal{F}_{y,z}) = \inf \mathcal{F}_{x,y} + \inf \mathcal{F}_{y,z} = d(x, y) + d(y, z),$$

so the map d is a pseudometric. Note that $d(ax, ay) = d(x, y)$, because $x^{-1}y = x^{-1}a^{-1}ay = (ax)^{-1}(ay)$, which implies that $f(x, y) = f(ax, ay)$ and

$$\mathcal{F}_{ax,ay} = \{f(x_1, x_2) + \cdots + f(x_k, x_{k+1}) \mid k \in \mathbb{N}, x_1 = ax, x_{k+1} = ay\}$$

$$= \{f(a^{-1}x_1, a^{-1}x_2) + \cdots + f(a^{-1}x_k, a^{-1}x_{k+1}) \mid k \in \mathbb{N}, x_1 = ax, x_{k+1} = ay\}$$

$$= \{f(x'_1, x'_2) + \cdots + f(x'_k, x'_{k+1}) \mid k \in \mathbb{N}, x'_1 = x, x'_{k+1} = y\} = \mathcal{F}_{x,y}.$$

Now, we must check that $\tau_d = \tau$, but everything reduces to work with local bases of the identity. In effect, we have

$$B(x, r) = \{y \in G \mid d(x, y) < r\} = x\{x^{-1}y \in G \mid d(1, x^{-1}y) < r\} = xB(1, r),$$

so for each point in G we can choose as local base in τ_d the family

$$\mathcal{B}'_x = \{xB(1, 2^{-n}) \subset G \mid n \in \mathbb{N}\}.$$

Then if we prove that for each $B \in \mathcal{B}$ there exists $B' \in \mathcal{B}'_1$ such that $B' \subset B$ and viceversa, we would have the same for any point of G, because by Lemma 7.5.1 $x\mathcal{B}$ is a local base of x in τ. From now on we will denote B'_k the ball of center 1 and radius 2^{-k}.

Let $x \in B_{i+1}$. From the definition of f it follows that $f(1, x) \leq 2^{-i-1}$, so $d(1, x) \leq 2^{-i-1} < 2^{-i}$, so $x \in B'_i$ and therefore $B_{i+1} \subset B'_i$ for i an arbitrary natural, which implies $\tau_d \subset \tau$.

For the other inclusion we must show that for all natural n there exists $i \in \mathbb{N}$ such that $B'_i \subset B_n$. Let $x \in B'_n$. We have $d(1, x) < 2^{-n}$, so there exists $k \in \mathbb{N}$ and $x_1, \ldots, x_{k+1} \in G$ with $x_1 = 1$ and $x_{k+1} = x$ such that

$$d(x_1, x_{k+1}) \leq f(x_1, x_2) + \cdots + f(x_k, x_{k+1}) < 2^{-n}.$$

We will prove by strong induction on k that in this situation $x_1^{-1}x_{k+1} \in B_n$, which would imply $1x \in B_n$ and $B'_n \subset B_n$, as desired.

The case $k = 1$ is trivial, because $f(x_1, x_2) < 2^{-n}$ implies that $f(x_1, x_2) \leq 2^{-n-1}$, so $x_1^{-1}x_2 \in B_{n+1} \subset B_n$. Assume now that it is true for each $i < k$ and let's prove the result for $k \geq 2$. Since f is nonnegative it is clear that $f(x_i, x_{i+1}) < 2^{-n}$ for $i = 1, \ldots, k$, so by induction we have $x_i^{-1}x_{i+1} \in B_{n+1}$. Moreover, $f(x_i, x_{i+1}) \leq 2^{-n-1}$ and for $i = 1$ we can distinguish two cases:

- Suppose that $f(x_1, x_2) = 2^{-n-1}$. Then it follows that

  $$f(x_2, x_3) + \cdots + f(x_k, x_{k+1}) < 2^{-n} - f(x_1, x_2) = 2^{-n} - 2^{-n-1} = 2^{-n-1}$$

  and by induction hypothesis $x_2^{-1}x_{k+1} \in B_{n+1}$. Hence,

  $$x_1^{-1}x_2x_2^{-1}x_{k+1} = x_1x_{k+1} \in B_{n+1}B_{n+1} \subset B_n.$$

- Suppose that $f(x_1, x_2) < 2^{-n-1}$. Choose the greatest j for which

  $$f(x_1, x_2) + \cdots + f(x_{j-1}, x_j) < 2^{-n-1}.$$

  If j equals k or $k+1$ we would have inmediately the result, because

  $$f(x_1, x_2) + \cdots f(x_{k-1}, x_k) < 2^{-n-1}$$

  and by induction hypothesis $x_1^{-1} x_k \in B_{n+1}$. Thus,

  $$x_1^{-1} x_k x_k^{-1} x_{k+1} = x_1 x_{k+1} \in B_{n+1} B_{n+1} \subset B_n.$$

  If $j < k$ we have by induction hypothesis $x_1^{-1} x_j = x_j \in B_{n+1}$ and

  $$f(x_1, x_2) + \cdots + f(x_j, x_{j+1}) \geq 2^{-n-1},$$

  so

  $$f(x_{j+1}, x_{j+2}) + \cdots + f(x_k, x_{k+1}) < 2^{-n} - 2^{-n-1} = 2^{-n-1}.$$

  This implies that $x_{j+1}^{-1} x_{k+1} \in B_{n+1}$. Finally, x_j, $x_j^{-1} x_{j+1}$ and $x_{j+1}^{-1} x_{k+1}$ are contained in B_{n+1} and we have

  $$x = x_1^{-1} x_{k+1} = x_{k+1} = x_j x_j^{-1} x_{j+1} x_{j+1}^{-1} x_{k+1} \in B_{n+1} B_{n+1} B_{n+1} \subset B_n$$

  by the second property of Lemma 7.6.2.

Since there are no more possible cases, we are done. $\square$

As the reader can see, the proof is constructive, yet the pseudometric we have defined is quite strange. An optimistic person may try to show that f generates τ, but in general it is not even a pseudometric.

Example 7.6.4. In $(\mathbb{R}, +, \tau_u)$ consider the decreasing local base

$$\mathcal{B} = \{B_1 = \mathbb{R}\} \bigcup \left\{ B_n = \left[-\frac{1}{3^n}, \frac{1}{3^n} \right] \subset \mathbb{R} \mid n \geq 2 \right\}.$$

It satisfies the properties of Lemma 7.6.2, because it is clearly symmetric and for $n \geq 2$ we have

$$B_{n+1} + B_{n+1} + B_{n+1} = 3 \cdot \left[-\frac{1}{3^{n+1}}, \frac{1}{3^{n+1}} \right] = \left[-\frac{1}{3^n}, \frac{1}{3^n} \right] \subset B_n.$$

However,

$$f\left(0, \frac{1}{9} + \frac{1}{27}\right) = \frac{1}{2}$$

and

$$f\left(0, \frac{1}{27}\right) + f\left(\frac{1}{27}, \frac{1}{9} + \frac{1}{27}\right) = \frac{1}{8} + \frac{1}{4} < \frac{1}{2},$$

so the triangle inequality does not hold.

Chapter 8

An introduction to profinite groups

Before starting this chapter it will be very useful recalling some basic topological results.

Proposition 8.0.1. *Let X be a Hausdorff topological space and let $Y \subseteq X$ be a compact subset. Then Y is closed.*

Proposition 8.0.2. *Let X be a compact topological space and let $Y \subseteq X$ be a closed subset of X. Then Y is compact.*

Proposition 8.0.3. *Let X be a Hausdorff topological space and let $Y, Z \subseteq X$ be two compact subsets of X. Then, there exist two open and disjoint subsets $U, V \subseteq X$ such that $Y \subseteq U$ and $Z \subseteq V$.*

Proposition 8.0.4. *Let $f\colon (X, \tau_X) \to (X', \tau_{X'})$ be a continuous mapping and let $Y \subseteq X$ be a compact subset of X. Then $f(Y)$ is compact.*

Proposition 8.0.5. *Let $f\colon (X, \tau_X) \to (X', \tau_{X'})$ be a continuous bijective map such that (X, τ_X) is a compact topological space and $(X', \tau_{X'})$ is Hausdorff. Then f is a homeomorphism.*

Proposition 8.0.6. *Let (X, τ) be a topological space and let $\{\mathcal{N}_x\}$ be a system of neighborhoods. Then (X, τ) is Hausforff if and only if for each $x \in X$ $\bigcap_{N \in \mathcal{N}_x} \overline{N} = \{x\}$.*

8.1 Inverse limits

In Chapter 6 we saw that the ring of p-adic integers can be seen as the set of coherent sequences (which we called the inverse limit) in the cartesian product $\prod_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$. In this chapter, we will generalize those concepts. First of all, we shall introduce the notion of directed set, which is the kind of index set that we are going to use to develop our theory. Of course, then $\mathbb{N}$ will be the first example of this new concept.

Definition 8.1.1. A *directed set* I is a partially ordered set (poset) with the property that for all $i, j \in I$, there exists $k \in I$ such that $k \geq i, j$.

Examples 8.1.2. (1) Clearly $\mathbb{N}$ with the usual order is a directed set.

(2) More generally, any linearly ordered (chain) set is trivially a directed set. However, not all directed sets are linearly ordered, as we shall later see (an example is given in Examples 8.1.4 (3)).

(3) Let X be any set and define $I = \{Y \subseteq X \mid Y \text{ is finite}\}$. Then, I ordered by inclusion is a directed set.

(4) Take a group G and let $\mathcal{N} = \{N \mid N \trianglelefteq G\}$. Then, $\mathcal{N}$ ordered by reverse inclusion is a directed set. Of course, it is equivalent to say that we order the subgroups according to the size of the quotients.

    More generally, we can take any family of normal subgroups $\mathcal{N}^* \subseteq \mathcal{N}$ satisfying the following property:

$$N, M \in \mathcal{N}^* \implies \exists K \in \mathcal{N}^* \text{ such that } K \subseteq N \cap M.$$

    Then, it is clear that $\mathcal{N}^*$ ordered by the reverse inclusion is also a directed set. There is a particular case of the last one which deserves our attention. Define

$$\mathcal{N}^* = \{N \trianglelefteq G \mid |G : N| < \infty\}.$$

    Let us show that the property above is satisfied. Indeed, recall the following fact from Group Theory: Let $H, K \leq G$ be two subgroups of a group G. Then,

$$|G : H \cap K| = |G : H||H : H \cap K| \leq |G : H||G : K|.$$

$$\begin{tikzcd}
& G \arrow[dl, dash] \arrow[dr, dash] & \\
H \arrow[dr, dash] & & K \arrow[dl, dash] \\
& H \cap K &
\end{tikzcd}$$

    Now, let $N, M \in \mathcal{N}^*$. Since $|G : N| < \infty$ and $|G : M| < \infty$, by the mentioned fact, it follows that $|G : N \cap M| < \infty$, and so $K := N \cap M \in \mathcal{N}^*$ is the required set. Hence $\mathcal{N}^*$ is a directed set.

Let us return for a moment to the ring $\mathbb{Z}_p$. Recall that we had the projection maps $\pi_n \colon \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$. The generalization of those maps is given in the next definition.

Definition 8.1.3. Let I be a directed set and assume that we have a family of sets, $\{X_i\}_{i\in I}$, together with a family of maps $\varphi_{ij}\colon X_i \to X_j$ for all $i \geq j$ satisfying:

(i) For all $i, j, k \in I$ such that $i \geq j$ and $j \geq k$, we have $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ (this is called a *compatibility condition*);

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

(ii) For all $i \in I$, the following holds: $\varphi_{ii} = \mathrm{id}_{X_i}$.

Then, we will say that the maps φ_{ij} are *connecting maps* and that $(X_i, \varphi_{ij})_{i,j\in I}$ is an *inverse system.*

Remark. In the particular case where the directed set is $I = \mathbb{N}$, assume that we have maps $\varphi_{m,m-1}\colon X_m \to X_{m-1}$ for all $m \geq 2$. Then, if we define $\varphi_{nm}\colon X_n \to X_m$ such that

$$\varphi_{nm} = \varphi_{n,n-1}\varphi_{n-1,n-2}\cdots\varphi_{m+1,m}$$

for all $n \geq m$, it is clear that $(X_i, \varphi_{nm})_{n,m\in\mathbb{N}}$ is an inverse system. Hence, there is a natural way to obtain an inverse system starting from consecutive projection maps.

Before continuing, we will give some examples in order to clarify the concept.

Examples 8.1.4. (1) Let $I = \mathbb{N}$ and $X_n = \mathbb{Z}/p^n\mathbb{Z}$, together with the projection maps $\pi_n\colon \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$ for all $n \geq 2$. By the previous remark, $(\mathbb{Z}/p^n\mathbb{Z}, \varphi_{nm})_{n,m\in\mathbb{N}}$ is an inverse system, where $\varphi_{nm}\colon \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ sends $x + p^n\mathbb{Z}$ to $x + p^m\mathbb{Z}$.

(2) Let G be a group and consider the directed set $\mathcal{N} = \{N \mid N \trianglelefteq G\}$ (see Examples 8.1.2 (4)). For all $N \geq_{\mathcal{N}} M$ (that is, $N \subseteq M$), define $\pi_{NM}\colon G/N \to G/M$ such that $\pi_{NM}(xN) = xM$. Then, it is trivial that $(G/N, \pi_{NM})_{N,M\in\mathcal{N}}$ is an inverse system.

Note that the maps π_{NM} are well-defined because $N \subseteq M$:

$$xN = yN \iff xy^{-1} \in N \subseteq M \implies xy^{-1} \in M \iff xM = yM.$$

(3) Take the group $(\mathbb{Z}, +)$ and define

$$\mathcal{N}^* = \{N \leq \mathbb{Z} \mid |\mathbb{Z} : N| < \infty\} = \{n\mathbb{Z} \mid n \in \mathbb{Z}\}$$

ordered, as always, by reverse inclusion. We have that

$$m\mathbb{Z} \leq_{\mathcal{N}} n\mathbb{Z} \iff n\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid n.$$

Hence, we can consider $I = \mathbb{N}$ as directed set, ordered by divisibility. We take the natural maps $\pi_{nm}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ such that $\pi_{nm}(x+n\mathbb{Z}) = x+m\mathbb{Z}$ for all $n\mathbb{Z} \geq_{\mathcal{N}} m\mathbb{Z}$ (again, they are well-defined because $n\mathbb{Z} \subseteq m\mathbb{Z}$). Then, $(\mathbb{Z}/n\mathbb{Z}, \pi_{nm})_{n,m\in\mathbb{N}}$ is an inverse system. Of course, in this case $\mathbb{N}$ is not a linearly ordered poset.

Until now, we have considered inverse systems consisting of some sets and connecting maps. Additionally, we can require the sets to be topological spaces, groups, or topological groups; and we can force the connecting maps to be continuous maps, group homomorphisms or continuous group homomorphisms, respectively. In these cases, we talk about inverse systems of topological spaces, inverse systems of groups or inverse systems of topological groups, respectively.

We are now ready to introduce one of the main concepts in this chapter:

Definition 8.1.5. Let $(X_i, \varphi_{ij})_{i,j\in I}$ be an inverse system of sets. Then, the *inverse limit* (or *projective limit*) of this inverse system is the set

$$\varprojlim_{i\in I} X_i = \left\{(x_i)_{i\in I} \in \prod_{i\in I} X_i \mid \varphi_{ij}(x_i) = x_j,\ \forall i \geq j\right\} \subseteq \prod_{i\in I} X_i.$$

The elements in the inverse limit are called *coherent tuples*.

Example 8.1.6. According to Theorem 6.6.5, it is clear that $\mathbb{Z}_p$ is isomorphic (as rings) and homeomorphic to the inverse limit $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ of the inverse system $(\mathbb{Z}/p^n\mathbb{Z}, \pi_{nm})_{n,m\in\mathbb{N}}$ recently described in Examples 8.1.4 (1).

For now on, we'll almost always assume that our inverse systems are inverse systems of topological spaces. Although one can think that we are losing too much, the reader should note that every set is a topological space when considered with the discrete topology. Hence, we are still working in all generality. Furthermore, the topology that we get in the inverse limit is by no means trivial (in many cases): the cartesian product of discrete spaces is not necessarily discrete when the index set is infinite.

Inverse limits also satisfy the so-called *universal property*. This universal property will soon be very important: in the next section, we will prove that actually it characterizes the inverse limit.

Proposition 8.1.7 (Universal property of the inverse limit)**.** *Let $(X_i, \varphi_{ij})_{i,j\in I}$ be an inverse system of topological spaces. Let Y be a topological space and assume that we have continuous maps $\psi_i\colon Y \to X_i$ for all $i \in I$ satisfying the compatibility condition $\psi_i\varphi_{ij} = \psi_j$ for all $i \geq j$. Then there exists a unique continuous map $\psi\colon Y \to \varprojlim_{i\in I} X_i$ such that the following diagram commutes:*

$$\begin{tikzcd}
 & \varprojlim_{i\in I} X_i \arrow[dr, "\varphi_i"] & \\
Y \arrow[ur, dashed, "\psi"] \arrow[rr, "\psi_i"] & & X_i
\end{tikzcd}$$

where φ_i denotes the ith coordinate projection π_i restricted to $\varprojlim_{i\in I} X_i$.

Proof. The only way to define φ making the diagram commutative is to take $\varphi\colon Y \to \varprojlim_{i\in I} X_i$ such that $\varphi(y) = (\psi_i(y))_{i\in I}$. Now, we have to check that it is continuous and that is is well-defined in the sense that $(\psi_i(y))_{i\in I} \in \varprojlim_{i\in I} X_i$.

On the one hand, for each $y \in Y$, by definition we have $(\psi_i(y))_{i\in I} \in \varprojlim_{i\in I} X_i$ if and only if $\varphi_{ij}(\psi_i(y)) = \psi_j(y)$ for all $i \geq j$, i.e., $\psi_i\varphi_{ij} = \psi_j$ for all $i \geq j$. The last expression holds because it is exactly the compatibility condition. Hence, $(\psi_i(y))_{i\in I} \in \varprojlim_{i\in I} X_i$.

Continuity is clear: ψ_i is continuous for all $i \in I$ and so φ is continuous in each component. Hence, φ is continuous in the product and thus it is also continuous in the subspace $\varprojlim_{i\in I} X_i$. $\square$

8.2 An alternative definition of the inverse limit

In this section we shall give an alternative approach to define the inverse limit, using the universal property described in Proposition 8.1.7.

Definition 8.2.1. Let $(X_i, \varphi_{ij})_{i,j\in I}$ be an inverse system of topological spaces. We say that a topological space X together with continuous maps $\varphi_i\colon X \to X_i$ which are compatible with the inverse limit (i.e. they satisfy $\varphi_i\varphi_{ij} = \varphi_j$ for all $i \geq j$) is the *inverse limit* of the inverse system if it satisfies the following universal property: for any topological space Y and for any family of continuous maps $\psi_i\colon Y \to X_i$ compatible with the inverse system (that is, $\psi_i\varphi_{ij} = \psi_j$ for all $i \geq j$), then there exists a unique continuous map $\psi\colon Y \to X$ such that $\psi\varphi_i = \psi_i$ for all $i \in I$, i.e., making the following diagram commutative:

$$\begin{tikzcd} & X \arrow[dr, "\varphi_i"] & \\ Y \arrow[ur, dashed, "\psi"] \arrow[rr, "\psi_i"] & & X_i \end{tikzcd}$$

The reader may have realized that in the previous definition there is something of which we have to be very careful: indeed, we are defining a new object in terms of a property (namely the universal property), and hence, the object might not be unique, or may not exist. Of course, we are now going to see that this new definition is entirely valid. What the following theorem basically says is that inverse limits always exist and are unique (up to homeomorphism).

Theorem 8.2.2. *Let $(X_i, \varphi_{ij})_{i,j\in I}$ be an inverse system of topological spaces. Then,*

(i) *The inverse limit (according to Definition 8.2.1) exists;*

(ii) *Any two inverse limits are homeomorphic.*

Proof. (i) In Proposition 8.1.7 we have seen that the set of coherent tuples satisfies the universal property of Definition 8.2.1. Hence, it is an inverse limit.

(ii) Assume that the topological spaces X (together with compatible continuous maps $\varphi_i \colon X \to X_i$ for all $i \in I$) and Y (together with compatible continuous maps $\psi_i \colon Y \to X_i$ for all $i \in I$) are two inverse limits of the inverse system $(X_i, \varphi_{ij})_{i,j \in I}$.

Since X satisfies the universal property, for the topological space Y and the compatible continuous maps ψ_i, there exists a unique continuous map $\psi \colon Y \to X$ such that the following diagram commutes:

$$\begin{tikzcd} & X \arrow[dr, "\varphi_i"] & \\ Y \arrow[ur, dashed, "\psi"] \arrow[rr, "\psi_i"] & & X_i \end{tikzcd}$$

Similarly, since Y also satisfies the universal property, for the topological space X and the compatible continuous maps φ_i, there exists a unique continuous map $\varphi \colon X \to Y$ making the following diagram commutative:

$$\begin{tikzcd} & Y \arrow[dr, "\psi_i"] & \\ X \arrow[ur, dashed, "\varphi"] \arrow[rr, "\varphi_i"] & & X_i \end{tikzcd}$$

Then, the map $\psi \circ \varphi \colon X \to X$ is continuous, since it is the composition of two continuous maps. Furthermore, the map $\mathrm{id}_X \colon X \to X$ is also continuous. Since the previous two diagrams commute, we have $\psi_i \circ \varphi = \varphi_i$ and $\varphi_i \circ \psi = \psi_i$, and so $\varphi_i \circ \psi \circ \varphi = \varphi_i$, for all $i \in I$. Hence we have two maps (namely $\psi \circ \varphi$ and id_X) such that the diagram below commutes:

$$\begin{tikzcd} & X \arrow[dr, "\varphi_i"] & \\ X \arrow[ur, dashed, bend left, "\psi\circ\varphi"] \arrow[ur, dashed, bend right, "\mathrm{id}_X"'] \arrow[rr, "\varphi_i"'] & & X_i \end{tikzcd}$$

By the uniqueness part of the universal property of X it follows that $\psi \circ \varphi = \mathrm{id}_X$. The same argument (just exchange X and Y) shows that $\varphi \circ \psi = \mathrm{id}_Y$. Hence, φ and ψ are mutually inverse, and thus bijective. We know that φ is bijective and continuous, and since $\varphi^{-1} = \psi$, it has continuous inverse, so it is a homeomorphism. $\square$

At this stage, we should stop for a moment to think of advantages and disadvantages of each of the two definitions of the inverse limit. On the one hand, Definition 8.1.5 is up to a point easier to understand, since it is much more explicit: inverse limits are no more than a subset of the cartesian product consisting of some special tuples, namely coherent tuples. On the other hand, Definition 8.2.1 is theoretically more interesting. Indeed, the concept of inverse limit is completely characterized by a universal property, which captures all its essence. Sometimes it will be more convenient to think of the inverse limit in the more down-to-earth way of the first definition, whereas other times it shall be very useful to work with the theoretical property of the second definition.

8.3 Properties of inverse limits

Let $\{X_i\}_{i\in I}$ be a collection of non-empty sets. Then, it is well-known that the cartesian product $\prod_{i\in I} X_i$ is also non-empty (in fact, this is equivalent to the axiom of choice). Unfortunately, the situation is not so good in the case of inverse limits. More precisely, if $(X_i, \varphi_{ij})_{i,j\in I}$ is an inverse system of non-empty sets, then $\varprojlim_{i\in I} X_i$ can be empty. This is shown in the next example.

Example 8.3.1. Take the directed set $I = \mathbb{N}$ (with the usual order) and $X_n = \mathbb{N}$ for all $n \in \mathbb{N}$. By the remark after Definition 8.1.3, it is enough to define connecting maps $\pi_n : X_{n+1} \to X_n$ for each $n \in \mathbb{N}$. Hence, let $\pi_n : \mathbb{N} \to \mathbb{N}$ such that $\pi_n(x) = 2x$. We claim that $\varprojlim_{n\in\mathbb{N}} X_n = \varnothing$. By contradiction, assume that $(x_n)_{n\in\mathbb{N}}$ is a coherent sequence. Write $x_1 = 2^k m$ with $2 \nmid m$ and k a non-negative integer. We have $2x_2 = \pi_1(x_2) = x_1 = 2^k m$ and so $x_2 = 2^{k-1}m$. Now, repeating k times, we clearly obtain $x_{k+1} = m$ and so $2x_{k+2} = \pi_{k+1}(x_{k+2}) = x_{k+1} = m$, which is impossible since $2 \nmid m$. Thus, the inverse limit is empty. Intuitively, at each step we are contracting $\mathbb{N}$ (note that the connecting maps π_n are not surjective for all $n \in \mathbb{N}$), and so, it is impossible to find a coherent sequence: once fixed the first element of the sequence, we can always go far enough to make the coherence condition impossible.

However, when the connecting maps are surjective, we have the following positive result.

Proposition 8.3.2. *Let $(X_i, \varphi_{ij})_{i,j\in\mathbb{N}}$ be an inverse system of non-empty sets where $\mathbb{N}$ is considered with its usual order. If φ_{ij} is surjective for each $i \geq j$, then*

$$\varprojlim_{n\in\mathbb{N}} X_n \neq \varnothing.$$

Proof. We are going to use that the directed set is $\mathbb{N}$ to build a coherent sequence inductively. Let $x_1 \in X_1 \neq \varnothing$. Now, take $x_2 \in X_2$ such that $\varphi_{21}(x_2) = x_1$ (note that we are using that φ_{21} is surjective). We continue in this fashion, obtaining a sequence $(x_n)_{n\in\mathbb{N}}$ which is coherent by construction, and so $\varprojlim_{n\in\mathbb{N}} X_n$ is non-empty, which is the desired conclusion. $\square$

During the proof we have also used two essential properties of $\mathbb{N}$: it is countable and well-ordered. As the following example shows, the surjectivity of connecting maps does not ensure nonemptiness in arbitrary directed sets.

Example 8.3.3. Consider the directed set $I = \{F \subseteq \mathbb{R} \mid \#F < \infty\}$ with usual inclusion. For every $F \in I$ define the set $X_F = \{f\colon F \to \mathbb{N} \mid f \text{ injective}\}$. If $F \supseteq F'$ ($F \geq F'$) define the map

$$\begin{aligned} \varphi_{F'F}\colon X_F &\to X_{F'} \\ f &\mapsto f|_{F'}. \end{aligned}$$

Then $(X_F, \varphi_{FF'})_{F,F' \in I}$ is clearly an inverse system of nonempty sets with surjective connecting maps, but the inverse limit is empty. Indeed, suppose by contradiction that there exists $(f_F)_{F \in I} \in \varprojlim_{F \in I} X_F$. For each real number x choose $F_x \in I$ containing it and define

$$\begin{aligned} g\colon \mathbb{R} &\to \mathbb{N} \\ x &\mapsto f_{F_x}(x). \end{aligned}$$

Let us prove that g does not depend on the choice of F_x. If $x \in F_1 \cap F_2$ then $x \in F_3 = F_1 \cup F_2 \in I$. Since $(f_F)_{F \in I}$ is a coherent tuple, it follows that

$$\varphi_{F_3 F_1}(f_{F_3}) = f_{F_3}|_{F_1} = f_{F_1}$$

and

$$\varphi_{F_3 F_2}(f_{F_3}) = f_{F_3}|_{F_2} = f_{F_2},$$

so $f_{F_1}(x) = f_{F_2}(x) = f_{F_3}(x)$. This also shows that if x and y are different real numbers then $g(x)$ and $g(y)$ are also different, because for any $F \in I$ containing both we have $g(x) = f_F(x)$ and $g(y) = f_F(y)$, but f_F is injective, so the images must be different. Thus, we have constructed an injective map from $\mathbb{R}$ to $\mathbb{N}$, which is impossible.

It is important to provide some examples of inverse limits.

Examples 8.3.4. (1) Given any topological space X and an arbitrary directed set I, consider $X_i = X$ for all $i \in I$. Then, $(X_i, \mathrm{id}_X)_{i \in I}$ is an inverse system.

Obviously, a coherent sequence will be just a constant sequence. Thus, the inverse limit is homeomorphic to the set X, by the map $\varphi\colon X \to \varprojlim X_i$ such that $\varphi(x) = (x)_{i \in I}$. That is,

$$\varprojlim_{i \in I} X_i \simeq X.$$

(2) Any cartesian product can be interpreted as an inverse limit. See Problem 24.

Now, we can state some interesting properties of inverse limits.

Theorem 8.3.5. *Let $\{X_i, \varphi_{ij}\}_{i \in I}$ be an inverse system of topological spaces.*

(i) *If all X_i are Hausdorff, then $\varprojlim_{i \in I} X_i$ is a closed subset of $\prod_{i \in I} X_i$.*

(ii) *If all X_i are non-empty, compact and Hausdorff, then $\varprojlim_{i \in I} X_i \neq \varnothing$.*

Proof. (i) For every $j \in I$, consider $L_j = \{(x_i)_{i\in I} \mid \varphi_{jk}(x_j) = x_k \;\; \forall k \leq j\}$. Then,

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

We shall prove that L_j is closed for any index. That is, given any $(x_i)_{i\in I} \in \prod_{i\in I} X_i \setminus L_j$ we shall find an open neighborhood W of $(x_i)_{i\in I}$ such that $W \cap L_j = \varnothing$. Notice that:

$$(x_i)_{i\in I} \notin L_j \iff \exists k \leq j \text{ such that } \varphi_{jk}(x_j) \neq x_k.$$

Furthermore X_k is Hausdorff, so there exist two open subsets $U_k, V_k \subseteq X_k$ which are disjoint such that $x_k \in U_k$ and $\varphi_{jk}(x_j) \in V_k$. Moreover, since the projection maps are continuous $U_j = \varphi_{jk}^{-1}(V_k)$ is an open subset such that $x_j \in U_j$. Thus, define

$$W = \prod_{i\in I} U_i \quad \text{where} \quad U_i = \begin{cases} U_j & \text{if } i = j \\ U_k & \text{if } i = k \\ X_i & \text{if } i \neq j, k, \end{cases}$$

is an open subset in the product topology which contains the sequence $(x_i)_{i\in I}$. Thus, W is an open neighbourhood of $(x_i)_{i\in I}$. Finally since $\varphi_{jk}(x_j) \notin U_k$, $W \cap L_j = \varnothing$.

Therefore each L_j is closed and $\varprojlim_{i\in I} X_i$ is closed, because it is the intersection of closed subsets.

(ii) First, we shall see that for any finite set $J = \{j_1, j_2, \ldots, j_n\}$ we have $\bigcap_{j\in J} L_j \neq \varnothing$. In the previous context consider, $j_0 = \max J$. Since the sets X_i are non-empty, $L_j \neq \varnothing$ for any $j \in I$, in particular $L_{j_0} \neq \varnothing$, so let $(x_i)_{i\in I} \in L_{j_0}$. Then $(x_i)_{i\in I} \in L_j$ for all $j \in J$. In fact, fix $j \in J$, then

$$\forall k \leq j \leq j_0 \quad \varphi_{jk}(x_j) = \varphi_{jk}(\varphi_{j_0 j}(x_{j_0})) = \varphi_{j_0 k}(x_{j_0}) = x_k \implies (x_i)_{i\in I} \in L_j.$$

Therefore, $(x_i)_{i\in I} \in \bigcap_{j\in J} L_j$ and $\bigcap_{j\in J} L_j \neq \varnothing$. Finally, according the Finite Intersection Property:

$$\varprojlim_{i\in I} X_i = \bigcap_{j\in J} L_j \neq \varnothing,$$

and we are done. □

Using this result we can give a new proof of Theorem 6.7.2.

Corollary 8.3.6. *Let $f(X) \in \mathbb{Z}_p[X]$. Then $f(X)$ has a root in $\mathbb{Z}_p$ if and only if it has roots in $\mathbb{Z}/p^n\mathbb{Z}$ for every $n \in \mathbb{N}$.*

Proof. The right implication was obvious, so we will go straight to $(\Leftarrow)$. For each $n \in \mathbb{N}$ define the set

$$X_n = \{x_n \in \mathbb{Z}/p^n\mathbb{Z} \mid \overline{f}(x_n) = \overline{0}\} \subseteq \mathbb{Z}/p^n\mathbb{Z}$$

and the maps φ_{nm} defined as in Examples 8.1.4 (1) but restricted to X_n. If n is greater than m it is clear that the image of any $x_n \in X_n$ through φ_{nm} is also a root of $f(X)$ in $\mathbb{Z}/p^m\mathbb{Z}$ so $\varphi_{nm}(X_n) \subseteq X_m$ and we can consider the inverse system $(X_n, \varphi_{nm})_{n,m\in\mathbb{N}}$. Since X_n is contained in $\mathbb{Z}/p^n\mathbb{Z}$ for each natural n the connecting maps are just restrictions of π_{nm}, the inverse limit of this system $\varprojlim_{n\in\mathbb{N}} X_n$ is a a subset of $\varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$ introduced in Examples 8.1.4 (1):

$$\begin{tikzcd}
\varprojlim \mathbb{Z}/p^n\mathbb{Z} \cdots \arrow[r] & \mathbb{Z}/p^n\mathbb{Z} \arrow[r, "\pi_n"] & \mathbb{Z}/p^{n-1}\mathbb{Z} \arrow[r] & \cdots \arrow[r] & \mathbb{Z}/p\mathbb{Z} \\
\varprojlim\limits_{n\in\mathbb{N}} X_n \cdots \arrow[r] \arrow[u, hook] & X_n \arrow[r, "\varphi_{nn-1}"] \arrow[u, hook] & X_{n-1} \arrow[r] \arrow[u, hook] & \cdots \arrow[r] & X_1 \arrow[u, hook]
\end{tikzcd}$$

By hypothesis the sets X_n are nonempty and finite, so endowed with discrete topology they are compact and Hausdorff topological spaces. Applying the previous theorem it follows that $\varprojlim_{n\in\mathbb{N}} X_n$ is nonempty. For any $x = (x_n)_{n\in\mathbb{N}}$ contained in $\varprojlim_{n\in\mathbb{N}} X_n \subseteq \mathbb{Z}_p$ we have

$$\begin{aligned}
f(x) \equiv f(x_n) \pmod{p^n} \quad \forall n \geq 1 &\implies f(x) \in p^n\mathbb{Z}_p \quad \forall n \geq 1 \\
&\implies f(x) \in \bigcap_{n\in\mathbb{N}} p^n\mathbb{Z}_p = \{0\},
\end{aligned}$$

so x is a root of $f(X)$ in $\mathbb{Z}_p$. $\square$

Corollary 8.3.7. *Let $(X_i, \varphi_{ij})_{i,j\in I}$ be an inverse system of non-empty, compact and Hausdorff topological spaces and fix $k \in I$. If the maps φ_{ik} are surjective for all $i \geq k$ then the projection map*

$$\varphi_k \colon \varprojlim_{i\in I} X_i \to X_k$$

is also surjective.

Proof. Let $x_k \in X_k$. For each $i \in I$ define the sets

$$Y_i = \begin{cases} X_i & \text{if } i < k, \\ \varphi_{ik}^{-1}(\{x_k\}) & \text{if } i \geq k. \end{cases}$$

Note that in both cases Y_i is nonempty (due to surjectiveness), compact and Hausdorff, because X_k is T_1 so $\{x_k\}$ is closed, thus $\varphi_{ik}^{-1}(\{x_k\})$ is closed in X_k and hence compact. Let us prove that $(Y_i, \varphi_{ij|_{Y_i}})_{i,j\in I}$ is an inverse system. As in the previous corollary, the conditions of the definition hold because we are just taking subsets and restrictions of an inverse system, but we have to show that if $i \geq j$ then $\varphi_{ij}(Y_i)$ is included in Y_j. If $j < k$ then $Y_j = X_j$ and the inclusion follows trivially. If $j \geq k$ then so is i. Let $y \in Y_i = \varphi_{ik}^{-1}(\{x_k\})$. By the compatibility condition we have

$$\begin{aligned}
\varphi_{jk} \circ \varphi_{ij}(y) = \varphi_{ik}(y) = x_k &\implies \varphi_{ij}(y) \in Y_j \\
&\implies \varphi_{ij}(Y_i) \subseteq \varphi_{jk}^{-1}(\{x_k\}) = Y_j.
\end{aligned}$$

Therefore, $(Y_i, \varphi_{ij|Y_i})_{i,j\in I}$ is an inverse system of nonempty compact and Hausdorff topological spaces, so by Theorem 8.3.5 $\varprojlim_{i\in I} Y_i$ is a nonempty subset of $\varprojlim_{i\in I} X_i$. Now, point that

$$Y_k = \varphi_{kk}^{-1}(\{x_k\}) = \mathrm{id}_{X_k}^{-1}(\{x_k\}) = \{x_k\},$$

so any coherent tuple inside $\varprojlim_{i\in I} Y_i$ has x_k at kth position. Since we can do this with any element of X_k, we conclude that φ_k is surjective. □

For instance, in Examples 8.1.4 (1) we are dealing with finite sets. Therefore, they are compact and Hausdorff (with discrete topology). Moreover, the connecting maps are surjective, so we have the surjectivity of all projections ensured.

Corollary 8.3.8. *Let $(X_i, \varphi_{i,j})_{i,j\in I}$ be an inverse system of compact and Hausdorff topological spaces, Y another compact and Hausdorff topological space and $\{\psi_i : Y \to X_i\}_{i\in I}$ a family of continuous maps compatible with the inverse system. If ψ_i is surjective for all $i \in I$ then the continuous map ψ given by the universal property is also surjective (see Proposition 8.1.7).*

Proof. See Problem 25. □

8.4 Profinite spaces

Definition 8.4.1. A topological space X is said to be a *profinite space* if it is the inverse limit of a family of finite spaces with the discrete topology.

Now we are going to state a theorem which allows us to recognize a profinite space, but we need a previous lemma.

Lemma 8.4.2. *Let X be a compact and Hausdorff topological space. Then the connected component of a point $x \in X$ is the intersection of all clopen subsets of X containing x.*

Proof. The proof of this lemma is done in Problem 4. □

Theorem 8.4.3. *Let X be a topological space. Then the following are equivalent:*

(i) *X is a profinite space.*

(ii) *X is compact, Hausdorff and totally disconnected.*

(iii) *X is compact, Hausdorff and there is a base for the topology consisting in clopen sets.*

Proof. (i) ⇒ (ii). Since X is a profinite space we have that $X = \varprojlim_{i\in I} X_i$ for some finite discrete topological spaces X_i. Then X_i are compact, Hausdorff and totally disconnected, for each $i \in I$. In Problem 1 it is proved that the properties of being Hausdorff and totally disconnected are preserved by the product and since both are also hereditary properties and $X = \varprojlim_{i\in I} X_i \subseteq \prod_{i\in I} X_i$ we get that X is Hausdorff and totally disconnected.

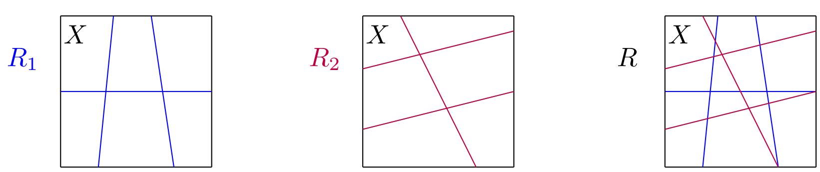
Let us prove now that X is compact. By Theorem 8.3.5, X is closed in $\prod_{i\in I} X_i$ which is a compact space by Tychonoff's Theorem and then by Proposition 8.0.2 we conclude that X is compact.

(ii) $\Rightarrow$ (iii). Given $x \in X$ and an open neighborhood W of x we have to see that there is a clopen neighborhood V of x which is contained in W. By the Lemma 8.4.2, since X satisfies the conditions in (ii), we have $\{x\} = C(x) = \bigcap_{i\in I} U_i$ where $\{U_i \mid i \in I\}$ is the family of all clopen subsets containing x. Now $X \smallsetminus W$ and $\bigcap_{i\in I} U_i = \{x\}$ are closed sets in X with empty intersection, hence, applying Lemma 6.7.1, we get that there exists a finite $J \subseteq I$ such that $(X \smallsetminus W) \cap (\bigcap_{j\in J} U_j) = \varnothing$. Therefore $V = \bigcap_{j\in J} U_j \subseteq W$ and V is the neigborhood of x we are searching for because it is clearly clopen (notice that the intersection is finite).

(iii) $\Rightarrow$ (i). Let us consider the family $\mathcal{R}$ of all equivalence relations R on X for which the corresponding equivalence classes are clopen subsets of X. In particular X/R carries the discrete topology. Besides, X is the disjoint union of the equivalence classes which are open by hypothesis, so these form a covering of X and since X is compact we have that there are finitely many equivalence classes. Thus X/R is finite.
We want to see X as an inverse limit so let us start showing that $\mathcal{R}$ is a directed set, in order to construct the inverse limit. We can consider the following partial order

$$R \geq R' \iff \forall x \in X,\ xR \subseteq xR'$$

that converts $\mathcal{R}$ into a directed set. In fact, for each $R_1, R_2 \in \mathcal{R}$, considering the partition R given by the intersection of the subsets in the partitions corresponding to R_1 and R_2, we have that $R \geq R_1$ and $R \geq R_2$. By way of clarification, we have the following picture expressing this idea.



Now we are going to prove that $X \cong \varprojlim_{R\in\mathcal{R}} X/R$. Consider the connecting maps

$$\begin{array}{rccc} \varphi_{RR'}: & X/R & \to & X/R' \\ & xR & \mapsto & xR'. \end{array}$$

They are well defined:

$$xR = yR \implies y \in xR \subseteq xR' \implies xR' = yR',$$

so $\{X/R, \varphi_{RR'}\}$ forms an inverse system. Now we are going to construct a homeomorphism $\psi\colon X \to \varprojlim_{R\in\mathcal{R}} X/R$ using the universal property. We need maps $\psi_R\colon X \to X/R$ which are compatible with the connecting maps, i.e., we search for ψ_R that makes the next diagram commutative:

$$\begin{tikzcd} X \arrow[r, "\psi_{R'}"] \arrow[d, "\psi_R"'] & X/R' \\ X/R \arrow[ur, "\varphi_{RR'}"'] & \end{tikzcd}$$

so we only have to consider ψ_R to be the continuous canonical map, i.e.,

$$\begin{array}{rccc} \psi_R\colon & X & \to & X/R \\ & x & \mapsto & xR. \end{array}$$

Now by the universal property there exists a unique continuous ψ defined as follows

$$\begin{array}{rccc} \psi\colon & X & \to & \varprojlim_{R\in\mathcal{R}} X/R \\ & x & \mapsto & (xR)_{R\in\mathcal{R}}. \end{array}$$

Besides, by Corollary 8.3.8, since ψ_R is surjective and X/R is compact and Hausdorff, we have that ψ is surjective.

Let us check now that it is injective. Given $x \neq y \in X$ we have to show that $\psi(x) \neq \psi(y)$. It is enough to prove that there is an equivalence relation $R \in \mathcal{R}$ (i.e. a partition of clopen sets) such that $xR \neq yR$. By hypothesis X is Hausdorff (in particular T_1) so there exists a neighborhood U of x such that $y \notin U$ and since there is a base of clopen sets for X, we can consider U to be clopen. Now $V = X \smallsetminus U$ is clopen and $y \in V$, so V is a neighborhood of y. Therefore we have a partition $X = U \cup V$ in clopen sets and this defines an equivalence relation $R \in \mathcal{R}$ for which $xR = U \neq V = yR$, concluding that ψ is injective.

Finally ψ is a continuous bijective map from a compact space X to $\varprojlim_{R\in\mathcal{R}} X/R$, which is Hausdorff, so by Proposition 8.0.5, ψ is a homeomorphism as we want to prove. $\square$

Theorem 8.4.4. *Let $X = \varprojlim_{i\in I} X_i$ be a profinite space. Then the following are equivalent:*

(i) *X is second countable.*

(ii) *X is a profinite space over a directed set which is countable with a total order.*

(iii) *X is a profinite space over $\mathbb{N}$ with the usual order.*

Proof. (iii) $\Rightarrow$ (ii). It is clear since $\mathbb{N}$ is countable and totally ordered.

(ii) $\Rightarrow$ (i). Suppose that J is countable with a total order and $X = \varprojlim_{j\in J} X_j$ with X_j finite discrete topological spaces. The topological space $\prod_{j\in J} X_j$ is second countable with countable basis

$$\beta = \{\prod_{j\in J} U_j \mid U_j = X_j \text{ for all but finitely many } j \in J,\ U_j \in \tau_j\}.$$

Using Proposition 3.3.3, we conclude that $X = \varprojlim_{j\in J} X_j \subseteq \prod_{j\in J} X_j$ is second countable.

(i) $\Rightarrow$ (iii). Consider $\mathcal{R}$ to be the family of all equivalence relations R on X for which the corresponding equivalence classes are clopen subsets of X, as in Theorem 8.4.3. We have a partition of X into finitely many clopen subsets, as we have seen in the theorem, and each xR, which is open, is a union of some of the elements in the countable basis of X. Therefore $\mathcal{R}$ is countable. Suppose $\mathcal{R} = \{R_1, R_2, \ldots\}$ which is not necessarily a linearly ordered set and for that reason define $\mathcal{R}' = \{R'_1, R'_2, \ldots\}$ by the rule $R'_i = R_1 \cap R_2 \cap \ldots \cap R_i$. Then $\mathcal{R}'$ is a directed set where the partial order is the following:

$$R'_i \geq R'_j \iff \forall x \in X,\ xR'_i \subseteq xR'_j \iff i \geq j$$

for each $i, j \in \mathbb{N}$. Now, following the same procedure to the one in the proof (iii) $\Rightarrow$ (i) of Theorem 8.4.3 with $\mathcal{R}'$ as the directed set, we get $X \cong \varprojlim_{R'\in\mathcal{R}'} X/R' = \varprojlim_{n\in\mathbb{N}} X/R'_n$. $\square$

8.5 Profinite groups

Definition 8.5.1. A *profinite group* G is an inverse limit of finite groups. In these finite groups we consider the discrete topology and so profinite groups are also topological groups.

If $G = \varprojlim_{i\in I} G_i$ where G_i are finite groups, we have that $G \leq \prod_{i\in I} G_i$ being the last one a topological group.

Examples 8.5.2. (1) Every finite group G is profinite corresponding to a constant inverse system (just consider G all the time).

(2) The cartesian product $\prod_{i\in I} G_i$, with G_i finite groups, is a profinite group for any indexed set I, by Examples 24 (2).

(3) The p-adic integers $\mathbb{Z}_p$ is a profinite group.

(4) In Problem 27 we shall see that

$$SL_2(\mathbb{Z}_p) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle|\ a, b, c, d \in \mathbb{Z}_p,\ \det A = 1 \right\}$$

is a profinite group because it is quite difficult to deduce it only from the definition.

Now we will prove the characterization theorem for profinite groups. Before proving it, it is necessary to present some concepts involving the core of a subgroup and the generation of topological subgroups.

8.5.1 Generation and core

Notation. Let G be a group and $X \subseteq G$. Then, for each natural number we define the *nth power of* X as

$$X^n = \{x_1 \dots x_n \mid x_i \in X \quad \forall i = 1, \dots, n\}.$$

On the other hand, the *inverse set of* X is defined as

$$X^{-1} = \{x^{-1} \mid x \in X\}.$$

We say that X is symmetric if $X^{-1} = X$.

Remark. If X is a symmetric subset of the group G; then $\langle X \rangle = \bigcup_{n \in \mathbb{N}} X^n$.

After these clarifications, we can define the core.

Proposition 8.5.3. *Let G be a group and let H be a subgroup (of finite index in G). Then, the subgroup*

$$H_G = \bigcap_{g \in G} H^g$$

is the largest normal subgroup of G contained in H (and has finite index over G). This subgroup is called the core *of H.*

Proof. Since H_G is the intersection of some subgroups of G, it is a subgroup of G.

For each $x \in G$ we have that

$$H_G^x = \bigcap_{g \in G} (H^g)^x = \bigcap_{g \in G} H^{gx} = \bigcap_{g \in G} H^g = H_G,$$

notice in the third equality we use that multiplying by a fixed element is a bijection. Therefore, H_G is a normal subgroup in G.

Futhermore, H_G is the largest normal subgroup contained in H. Consider a normal subgroup $N \trianglelefteq G$ such that $N \subseteq H$, then for any $g \in G$ we have that:

$$N = N^g \subseteq H^g \implies N \subseteq \bigcap_{g \in G} H^g = H_G.$$

Finally, we shall prove that if the original group has finite index the core will have finite index. If we prove that the set of conjugates has finite order it follows.

Cosets form a disjoint partition of the group G, i.e., $G = \cup_{i=1}^{n} Hg_i$. Hence, for any $g \in G$, there exist some $h \in H$ and $i \in \{1, \ldots, n\}$ such that $g = hg_i$. Thus,

$$H^g = H^{hg_i} = H^{g_i}.$$

Therefore, it obvious that the set of conjugates is finite, that is,

$$\{H^g \mid g \in G\} = \{H^{g_i} \mid i = 1, \ldots, n\}.$$

On the other hand the conjugation by any $g \in G$ is an automorphism in G, so the indexes are preserved, i.e., $|G : H| = |G : H^g|$.

Thus, we have this upper bound for the core:

$$|G : H_G| = \left| G : \bigcap_{i=1}^{n} H^{g_i} \right| \leq \prod_{i=1}^{n} |G : H^{g_i}| = |G : H|^{|G:H|}$$

and so the index of the core is finite. □

It can be proved that a better bound for the index of the core H_G in G is given by the factorial $|G : H|!$. Other interesting property of the core states that if the original subgroup H is open, then the core will also be open.

Lemma 8.5.4. *Let G be a compact topological group and H an open subgroup of G. Then, the core of H is a normal open subgroup of G.*

Proof. By construction the core is a normal subgroup. Furthermore, for each $g \in G$ conjugation is a homeomorphism, so H^g is open. Hence, the core is the intersection of open subgroups. The proof is completed by showing that the transversals set is finite. However, G is a compact topological space and H is an open subgroup. Therefore, according to Lemma 7.1.8 $|G : H|$ is finite, and the core is the finite intersection of open subsets, so it is open. □

In the same way having a subgroup H in a topological group G, one can define the smallest normal subgroup of G containing the subgroup H. This subgroup is called the *normal clousure* of H and it is denoted by H^G. The normal clousure is defined as following:

$$H^G = \langle H^g \mid g \in G \rangle.$$

We may only need the core, so we leave it for the reader to verify that the equivalent of Lemma 8.5.1 is true for the normal clousure.

We can now formulate the main results concercing the generation of topological subgroups.

Lemma 8.5.5. *Let G be a topological group and let X be an open subset in G. Then, $\langle X \rangle$ is open.*

Proof. According to one above remark, when X is symmetric we have that

$$\langle X \rangle = \bigcup_{n \in \mathbb{N}} X^n.$$

Since X is open, X^n is also open for any natural number. Therefore, since $\langle X \rangle$ is the union of open subsets, it is open.

When X is not symmetric, $Y = X \cup X^{-1}$ is symmetric and we shall see that it is open. In fact, since X is open, X^{-1} is open and so it is the union. Finally, by the first part of the proof $\langle X \rangle = \langle Y \rangle = \bigcup_{n \in \mathbb{N}} Y^n$ is open. This finishes the proof. □

The analogue result is not held for closed subsets, i.e., if X is closed, then $\langle X \rangle$ is not necessarily closed. The following counter-example confirms the assertion.

Example 8.5.6. Consider the complete topological group $(\mathbb{Z}_p, +)$ and the closed subset $\{1\}$ (note that $\mathbb{Z}_p$ is T_1, so singletons are closed).

Then, $\langle 1 \rangle = \mathbb{Z} \leq \mathbb{Z}_p$. Nevertheless, by 6.5.5 $\overline{\mathbb{Z}} = \mathbb{Z}_p$, which is not countable, but $\mathbb{Z}$ is countable. Thus, $\overline{\mathbb{Z}} \neq \mathbb{Z}$ and so $\langle 1 \rangle = \mathbb{Z}$ is not closed.

8.5.2 Profinite groups' characterization theorem

Now we are going to recall some results about openness and closedness of subgroups of a topological group, where we denote by $H \leq_o G$ an open subgroup H in G and by $H \leq_c G$ a closed subgroup H in G:

(1) If $H \leq_o G$, then $H \leq_c G$.

(2) $H \leq_c G$ and $|G\colon H| < \infty$, then $H \leq_o G$.

(3) If G is compact and $H \leq_o G$, then $|G\colon H| < \infty$.

Taking into consideration these three results we have the following:

(4) If G is compact, then $H \leq_o G$ if and only if $H \leq_c G$ and $|G\colon H| < \infty$.

There is a very deep question: If G is a profinite group and $H \leq G$ such that $|G\colon H| < \infty$, is $H \leq_o G$? The answer is positive if G is "finitely generated"(we will see this concept later). This generalizes a question of Serre and was solved recently by Nikolov-Segal.

We now prove the main theorem in this section.

Theorem 8.5.7 (Characterization of profinite groups)**.** *Let G be a topological group. Then the following are equivalent:*

(i) *G is a profinite group.*

(ii) *G is compact, Hausdorff and totally disconnected.*

(iii) *G is compact and there exists a fundamental system of neighborhoods $\mathcal{N}$ of 1 consisting of open normal subgroups and such that $\bigcap_{N\in\mathcal{N}} N = \{1\}$.*

(iv) *There exists a fundamental system of neighborhoods $\mathcal{N}$ of 1 consisting of open normal subgroups and such that $G \cong \varprojlim_{N\in\mathcal{N}} G/N$.*

There are two equivalent conditions (iii') *to* (iii) *and* (iv') *to* (iv) *which are the following:*

(iii') *G is compact and all open normal subgroups of G are a fundamental system of neighborhoods of 1 intersecting in $\{1\}$.*

(iv') *All open normal subgroups of G are a fundamental system of neighborhoods of 1 and $G \cong \varprojlim_{N\trianglelefteq_o G} G/N$.*

Proof. We will proceed in the usual way of proving implication chains.

(i) $\Rightarrow$ (ii). G is a profinite group, so it is a profinite topological space. Therefore, by Theorem 8.4.3, G is compact, Hausdorff and totally disconnected.

(ii) $\Rightarrow$ (iii). From being G a profinite space, there exists a basis for the topology consisting on clopen sets. Consider from these clopen sets, those which contain 1. That is a fundamental system of neighborhoods of 1. Since G is Hausdorff and the neighborhoods are closed, by Proposition 8.0.6 the intersection of these neighborhoods of 1 is $\{1\}$.

Using Theorem 8.4.3, the task is now to prove that for each clopen neighborhood of 1, V, there exists an open normal subgroup of G, $N \trianglelefteq_o G$, such that $1 \in N \subseteq V$. We will prove this statement in a constructive way.

Let V be a clopen neighborhood of 1 and consider any $x \in V$. On the one hand, in any topological group the multiplicative map is continuous, so $\mu^{-1}(V)$ is open in $G\times G$. On the other hand, since $\mu(x,1) = x$, $(x,1) \in \mu^{-1}(V)$.

Therefore $\mu^{-1}(V)$ is an open subset in $G\times G$ containing $(x,1)$, so there exist two open sets, V_x and S_x, in G such that $x \in V_x \subseteq V$ and $1 \in S_x \subseteq V$. Now, since $V = \bigcup_{x\in V} V_x$, the family $\{V_x \mid x \in V\}$ is an open covering of V, which is closed in the compact topological space G, and so V is compact. Then, we can obtain a finite subcovering,

$$V = \bigcup_{x\in V} V_x = \bigcup_{i=1}^{r} V_{x_i}.$$

Now define $S = \bigcap_{i=1}^{r} S_{x_i}$, for which $VS \subseteq V$. Consider the symmetric set $X = S \cup S^{-1}$ which is still open, contained in V and satysfies that $VX \subseteq V$. Thus, for any natural number

$$VX^n = VX \overset{n}{\cdots} X \subseteq V \implies V\langle X\rangle \subseteq V.$$

Finally, we have an open subgroup $\langle X \rangle$ (since X is open, using Lemma 8.5.5) in G such that $V\langle X \rangle \subseteq V$, and so $\langle X \rangle \subseteq V$, because $1 \in V$.

The only point remaining concerns the normality, but according to Lemma 8.5.4 the core of the open subgroup $\langle X \rangle$, $N = \langle X \rangle_G \trianglelefteq_o G$ is a normal open subgroup contained in $\langle X \rangle$ and hence in V. Thus, we are done.

(iii) $\Rightarrow$ (iv). For each normal subgroup N consider the canonical projection $\pi_N \colon G \to G/N$ and the natural connecting maps of the inverse limit $\pi_{NM} \colon G/N \to G/M$ such that $\pi_{NM}(gN) = gM$ (for all $N \subseteq M \in \mathcal{N}$).

Combining these maps, we obtain the following continuous homomorphism

$$\begin{aligned} \pi \colon G &\to \varprojlim_{N \in \mathcal{N}} G/N \\ g &\mapsto (gN)_{N \in \mathcal{N}}. \end{aligned}$$

Since each of the canonical projections is a continuous homomorphism, so it is the map π. Moreover, each of the canonical projections is a epimorphism, so π is onto.

On the other hand, π is injective. Since, π is a group homomorphism, we are reduced to computing the kernel.

$$\begin{aligned} g \in \ker \pi &\iff \pi(g) = (N)_{N \in \mathcal{N}} \iff gN = N \quad \forall N \in \mathcal{N} \\ &\iff g \in N \quad \forall N \in \mathcal{N} \iff g \in \bigcap_{N \in \mathcal{N}} N = \{1\} \iff g = 1. \end{aligned}$$

Hence, $\ker \pi = \{1\}$ and so π is injective.

Thus, π is a bijective, continuous group homomorphism. Finally, π^{-1} is also continuous. In fact, π is a continuous bijective map, G is a compact topological space and by assumption $\varprojlim_{N \in \mathcal{N}} G/N$ is Hausdorff, so by Proposition 8.0.5, π is a homeomorphism and a group-isomorphism, i.e., π is a isomorphism of topological groups.

(iv) $\Rightarrow$ (i). This implication is straightforward from the definition of profinite group. It remains to prove that G/N has the discrete topology for each $N \in \mathcal{N}$.

Since N is an open subgroup and its canonical projection π_N is continuous, $\pi_N^{-1}(\{x\}) = xN = r_x(N)$ is open for any $x \in G$. Therefore, any singleton is open in G/N and so we have the discrete topology. $\square$

Example 8.5.8. Let us show that the ring of p-adic integers $\mathbb{Z}_p$ verifies (iii') and (iv') of Theorem 8.5.7. Firstly, we proved that $\mathbb{Z}_p$ is compact and secondly, since $p^n\mathbb{Z}_p$ are open normal subgroups for each $n \in \mathbb{N}$ and we saw that they are balls around the identity, then they form a fundamental system of neighborhoods of 1 and clearly $\bigcap_{n\geq 1} p^n\mathbb{Z}_p = \{0\}$, so (iii') is satisfied. Now, we also proved that $\mathbb{Z}_p \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}_p$, therefore (iv') is satisfied.

8.5.3 Consequences

Some properties, which are not held in general topological groups, are true in profinite groups. Now, we will introduce some of them.

Lemma 8.5.9. *Let G be a profinite group and let X, Y be two closed subsets of G. Then, XY is closed.*

Proof. Since G is a profinite group, G is a compact and Hausdorff topological space, so X and Y are compact subsets in G. On the other hand, the multiplicative map is continuous in any topological group and so it preserves the compactness. Therefore, XY is compact in the compact space G and hence it is closed. □

The equivalent of the previous lemma is not true for general topological groups, as one can see in Exercise 23.

Lemma 8.5.10. *Let G a profinite group and let H be a subgroup of G. Then, H is a profinite subgroup if and only if H is closed in G.*

Proof. Since G is a profinite group, by Theorem 8.5.7, G is compact, T_2 and totally disconnected. Futhermore, any subgroup H of G is also T_2 and totally disconnected, so we are reduced to the compactness issue.

Since G is a compact and Hausdorff topological space, the subgroup H is compact if and only if H is closed. Hence, the subgroup H is a profinite subgroup if and only if it is closed. □

Lemma 8.5.11. *Let G a profinite group and let N be a normal open subgroup of G. Then, G/N is a profinite group if and only if N is closed in G.*

Proof. Exercise 26. □

8.6 Properties of profinite groups

The following proposition gives a method to compute topological closures using only algebraic operations.

Proposition 8.6.1. *Let G be a profinite group and $\mathcal{N}$ a fundamental system of neighborhoods of 1 consisting of open normal subgroups such that $\bigcap_{N\in\mathcal{N}} N = \{1\}$. Then for every $X \subseteq G$,*

$$\overline{X} = \bigcap_{N\in\mathcal{N}} XN.$$

Proof. For one inclusion, let $N \in \mathcal{N}$. Since G is profinite, it is compact by Theorem 8.5.7 and since N is open, using Proposition 7.1.8, the index $|G : N|$ is finite. Then the union $XN = \bigcup_{x \in X} xN$ is finite, and being a finite union of closed sets (note that N is also closed by Proposition 7.1.6), it is closed. Hence, the intersection $\bigcap_{N \in \mathcal{N}} XN$ is closed and contains X (because $X = X \cdot 1 \subseteq XN$). Therefore, $\overline{X} \subseteq \bigcap_{N \in \mathcal{N}} XN$.

We now prove the opposite inclusion. Let $g \in \bigcap_{N \in \mathcal{N}} XN$. Recall that $g\mathcal{N}$ is a fundamental system of neighborhoods of g (see Lemma 7.5.1). Hence, in order to see that $g \in \overline{X}$ it is enough to show that $gN \cap X \neq \varnothing$ for all $N \in \mathcal{N}$. Fix $N \in \mathcal{N}$. Since $g \in \bigcap_{N \in \mathcal{N}} XN$, in particular $g \in XN$, i.e. there exists $x \in X$ such that $g \in xN$, and thus $x \in xN = gN$ from which follows that $x \in gN \cap X$. We conclude that the intersection is non-empty as we wanted to prove. □

We can also compute closures using inverse limits. We provide this new method in the following proposition, but before we need a lemma.

Lemma 8.6.2. *Let $G = \varprojlim_{i \in I} G_i$ be a profinite group and denote by $\varphi_i \colon G \to G_i$ the restriction to G of projection homomorphisms for each $i \in I$. Then $\mathcal{N} = \{\ker \varphi_i\}_{i \in I}$ is a fundamental system of neighborhoods of 1 consisting of open normal subgroups such that $\bigcap_{i \in I} \ker \varphi_i = \{1\}$.*

Proof. Firstly, the kernel of a group-homomorphism is always normal. Moreover, for each $i \in I$, the homomorphisms $\varphi_i \colon G \to G_i$ are continuous, and since $\{1\}$ is open in G_i (note that we are working with the discrete topology), we have that $\ker \varphi_i = \varphi_i^{-1}(1)$ is open.

We now prove that $\mathcal{N} = \{\ker \varphi_i\}_{i \in I}$ is a fundamental system of neighborhoods. To do so, let

$$N(j) = \prod_{i \in I} X_i \cap G \quad \text{where} \quad X_i = \begin{cases} G_i & \text{if } i \neq j, \\ \{1\} & \text{if } i = j. \end{cases}$$

Denote by $\pi_j \colon \prod_{i \in i} G_i \to G_j$ the jth coordinate projection. Then, we have

$$\ker \varphi_j = \ker \pi_j \cap G = N(j)$$

for all $j \in I$. Therefore, if we prove that $\mathcal{N} = \{N(j) \mid j \in I\}$ is a fundamental system of neighborhoods of 1, then we are done. It is clear that $\mathcal{N}$ is not a fundamental system of neighborhoods of 1 in the full cartesian product. However, in the topology induced in G it is a fundamental system of neighborhoods. Indeed, let M be a neighborhood of 1 in G. Then, there exists M' a neighborhood of 1 in the full cartesian product such that $M = M' \cap G$. Morever, there exists a basic open set containing 1 inside M', say

$$\prod_{i \in I} Y_i, \quad \text{where} \quad Y_i = \begin{cases} G_i & \text{if } i \neq j_1, \dots, j_k, \\ \{1\} & \text{otherwise.} \end{cases}$$

Since I is a directed set, let $j_0 \geq j_1, \dots j_k$. Let us prove that

$$N(j_0) \subseteq G \cap \prod_{i \in I} Y_i.$$

Let $(x_i)_{i\in I} \in N(j_0)$. From the definition of $N(j_0)$ it follows that $x_{j_0} = 1$ and since $(x_i)_{i\in I} \in G$ and all connecting maps are group-homomorphisms, we have $1 = \varphi_{j_0 j}(1) = x_j$ for all $j \leq j_0$. In particular $x_{j_1}, \dots, x_{j_k} = 1$ and so $(x_i)_{i\in I} \in G \cap \prod_{i\in I} Y_i$. Then

$$N(j_0) \subseteq G \cap \prod_{i \in I} Y_i \subseteq G \cap M' = M$$

and $\mathcal{N}$ is a fundamental system of neighborhoods of 1. It is clear that the intersection of all of them is $1 = (1)_{i\in I}$. $\square$

Proposition 8.6.3. *Let $G = \varprojlim_{i\in I} G_i$ be a profinite group and take $X \subseteq G$. Then,*

$$\overline{X} = \varprojlim_{i \in I} \varphi_i(X).$$

Proof. Since $\overline{X} \subseteq \varprojlim_{i\in I} \varphi_i(\overline{X})$, there exists the obvious inclusion map:

$$\begin{array}{rccc} \iota\colon & \overline{X} & \to & \varprojlim_{i\in I} \varphi_i(\overline{X}) \\ & x & \mapsto & \iota(x) = x. \end{array}$$

Notice that for each $i \in I$, $\varphi_i(\overline{X})$ is compact and Hausdorff. In fact, $\overline{X} \leq_c G$, which is a compact topological space, so $\overline{X}$ is compact in G and φ_i is continuous, hence $\varphi_i(\overline{X})$ is compact. Futhermore, we also have that $\overline{X}$ is compact and Hausdorff. Therefore, $\{\varphi_i\}_{i\in I}$ is trivially compatible and continuous map family. Moreover, each map is onto when restricted to the image, i.e. when considered that $\varphi_i \colon \overline{X} \to \varphi_i(\overline{X})$.

Finally, ι is the unique map given by the universal property for which the following diagram commutes:

$$\begin{tikzcd} & \varprojlim_{i\in I} \overline{X} \arrow[dr, "\varphi_i"] & \\ \overline{X} \arrow[ur] \arrow[rr, "\varphi_i"] & & \varphi_i(\overline{X}) \end{tikzcd}$$

Thus, by Problem 8.3.8 ι is onto and hence $\varprojlim_{i\in I} \overline{X} = \overline{X}$.

Therefore, if we prove that $\varphi_i(\overline{X}) = \varphi_i(X)$ for all $i \in I$, then we are done. The inclusion $\varphi_i(\overline{X}) \supseteq \varphi_i(X)$ is clear so let us prove the opposite one. Let $g \in \overline{X}$. Using Proposition 8.6.1 and Lemma 8.6.2 together, we obtain that

$$\overline{X} = \bigcap_{i\in I} X \ker \varphi_i.$$

Thus, we can write $g = x_i y_i$ with $x_i \in X$ and $y_i \in \ker \varphi_i$ for all $i \in I$. Then

$$\varphi_i(g) = \varphi_i(x_i y_i) = \varphi_i(x_i)\varphi_i(y_i) = \varphi_i(x_i) \in \varphi_i(X)$$

and the conclusion follows.

$\square$

Given a profinite group, we still haven't seen any method to decide whether it is metrizable or not (apart from the general results from Topology or Topological Groups, see for example Theorem 3.4.7). Fortunately, the situation is particularly easy for profinite groups, as the following theorem shows.

Theorem 8.6.4. *Let G be a profinite group. Then the following are equivalent:*

(i) *G is metrizable;*

(ii) *G is second countable;*

(iii) *G is first countable;*

(iv) *$G \cong \varprojlim_{n\in\mathbb{N}} G_n$ where G_n are finite groups.*

(v) *G has a descending chain of open normal subgroups $N_1 \supseteq N_2 \supseteq \cdots$ which forms a fundamental system of neighborhoods of 1 such that $\bigcap_{i=1}^{\infty} N_i = \{1\}$.*

Proof. (i) $\Rightarrow$ (iii). This is also a general result of topology, see Examples 3.2.3.

(iii) $\Rightarrow$ (i). G is a first countable topological group, so by Theorem 7.6.3 it is pseudometrizable, and so there exists a pseudometric d. Moreover, since G is Hausdorff, for each $x \neq y \in X$ there exists $r > 0$ such that $x \notin B(y, r)$ and $y \notin B(x, r)$. Hence, $d(x, y) > r > 0$ and d is a metric, i.e. G is metrizable.

(v) $\Rightarrow$ (iii). Let $\mathcal{N}$ be a descending fundamental system of neighborhoods of 1 consisting of open normal subgroups whose intersection is trivial. Write $\mathcal{N} = \{N_n \mid n \in \mathbb{N}\}$. By Theorem 8.5.7, we have $G \cong \varprojlim_{n\in\mathbb{N}} G/N_n$ (since for each $n \in \mathbb{N}$ we have that N_n is open and G is compact, the index $|G : N_n|$ is finite and so the groups G/N_n are finite).

(iii)$\Rightarrow$(v). As in the proof of (iii)$\Rightarrow$(iv), let $\mathcal{N}'' = \{N_n \mid n \in \mathbb{N}\}$ be a countable fundamental system of neighborhoods of 1 consisting of open normal subgroups which intersect at $\{1\}$. Now, define

$$\mathcal{N}^* = \{N_1 \cap N_2 \cap \cdots \cap N_n \mid n \in \mathbb{N}\}.$$

Since the inetrsection of normal subgroups is normal, $\mathcal{N}*$ is a fundamental system of neighborhoods of 1 consisting of open normal subgroups such that the intersection is $\{1\}$ (by Proposition 8.0.6). Moreover, the system is descending and so (v) holds.

x (ii) $\Rightarrow$ (iii). This is a general fact about topology explained in the comments after Definition 3.3.1.

(iii) $\Rightarrow$ (iv). Since G is first countable, let $\mathcal{N}$ be a countable fundamental system of neighborhoods of 1. By Theorem 8.5.7, there also exists a fundamental system of neighborhoods of 1, say $\mathcal{N}'$, consisting of open normal subgroups such that $\bigcap_{N\in\mathcal{N}'} N = \{1\}$.

Now, we are going to build a countable fundamental system of neighborhoods of 1 consisting of open normal subgroups such that they intersect at $\{1\}$. For each $N \in \mathcal{N}$ choose $M_N \in \mathcal{N}'$ such that $M_N \subseteq N$. Then it is clear that the family

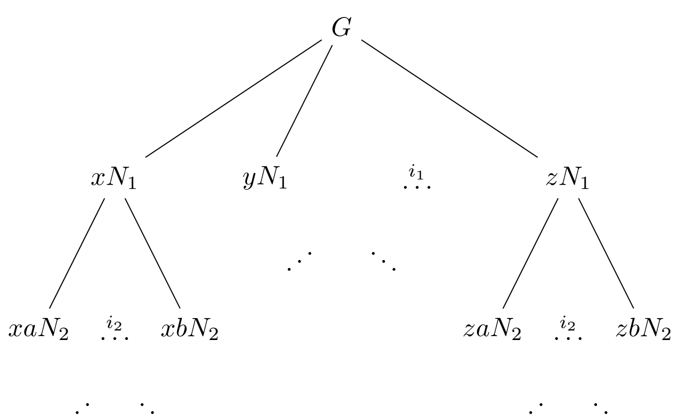
$$\mathcal{N}'' = \{M_N \mid N \in \mathcal{N}\}$$

is a countable fundamental system of neighborhoods of 1 consisting of open normal subgroups. Furthermore, Proposition 8.0.6 tells us (note that all M_N are also closed, by Proposition 7.1.6) that we have that $\bigcap_{N\in\mathcal{N}''} N = \{1\}$ and so $\mathcal{N}''$ is the desired countable basis of 1. By Theorem 8.5.7, it follows that $G \cong \varprojlim_{n\in\mathbb{N}} G_n$ where G_n are finite groups.

(iv) $\Rightarrow$ (ii). Profinite groups are in particular profinite spaces, so this implication follows by Theorem 8.5.7.

$\square$

Remark. Assume that G is a metrizable profinite group. Then, we will see that it is actually metrizable by an ultrametric. By the previous theorem, let $\mathcal{N}$ be a descending chain of neighborhoods $G \supseteq N_1 \supseteq \cdots \supseteq N_k \supseteq \ldots$ satisfying $\bigcap_{k\geq 1} N_k = \{1\}$. We can then consider the so-called *coset-tree*:



Similarly as in Example 6.1.14 it can be seen that the infinite paths of the tree are in one-to-one correspondence with G and that an ultrametric can be defined in the tree. An adequate choice of the distance makes the bijection an isometry and hence G is an ultrametric space.

This example closes the circle in the following sense: we started building profinite groups inspired by the ring of p-adic integers, which is an ultrametric space. Now, it turns out that every metrizable profinite group is an ultrametric space.

8.7 Convergence and completeness in profinite groups

We have already seen some properties of metrizable profinite groups. Nevertheless, even in the case of a non-metrizable profinite group it's not all bad news.

Recall that in a general topological space the situation is not very good: it is impossible to talk about Cauchy sequences, uniform continuity... (see the Introduction in Chapter 4). We need a metric space (or at least a uniform space) for those concepts to make sense. However, profinite groups (doesn't matter if they are metrizable or not) allow us to generalize and to use concepts such as the previous ones (for example Cauchy sequences) as if we were working in a metric space.

First we analyze Cauchy sequences in a general topological group. Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in a topological group and $\mathcal{N}$ a fundamental system of neighborhoods of 1. We say that a sequence is *left-Cauchy* if

$$\forall U \in \mathcal{N}\ \exists n_0 \in \mathbb{N} \text{ such that } \forall n, m \geq n_0,\ x_n \in Ux_m.$$

We define *right-Cauchy* sequences in a completely analogue way. If a sequence is both left- and right-Cauchy, we shall say that it is a Cauchy sequence. This is why in a general topological group it is impossible to talk about Cachy sequences. Note that if our neighborhoods were normal subgroups, then the definitions of left-Cauchy and right-Cauchy sequences coincide, and so we can directly speak about Cauchy sequences. The existence of such fundamental system of neighborhoods is guaranteed in profinite groups, and hence this motivates the definition of Cauchy sequences (actually Cauchy nets, which is a more general concept) in profinite groups. First we give a couple of general definitions and then we concentrate on profinite groups.

Definition 8.7.1. A *net* in a topological space X is a tuple $(x_i)_{i\in I}$ where I is a directed set and $x_i \in X$ for all $i \in I$.

Definition 8.7.2. Let X be a topological space and $\mathcal{N}_x$ a complete or fundamental system of neighborhoods. We say that a net $(x_i)_{i\in I}$ in X *converges* to x if

$$\forall U \in \mathcal{N}_x\ \exists i_0 \in I \text{ such that } \forall i \geq i_0,\ x_i \in U.$$

It can be proved (but we are not going to do so) that continuity of maps between topological spaces can be characterized using convergence of nets.

Definition 8.7.3. Let G be a profinite group and $\mathcal{N}$ a fundamental system of neighborhoods of 1 consisting of open normal subgroups such that $\bigcap_{N\in\mathcal{N}} N = \{1\}$. A net $(x_i)_{i\in I}$ in G is said to *converge* to x if

$$\forall N \in \mathcal{N}\ \exists i_0 \in I \text{ such that } \forall i \geq i_0,\ x_i \in xN (= Nx).$$

Definition 8.7.4. Let G be a profinite group and $\mathcal{N}$ a fundamental system of neighborhoods of 1 consisting of open normal subgroups such that $\bigcap_{N\in\mathcal{N}} N = \{1\}$. A net $(x_i)_{i\in I}$ in G is said to be *Cauchy* if

$$\forall N \in \mathcal{N}\ \exists i_0 \in I \text{ such that } \forall i,j \geq i_0,\ x_i \in x_j N \text{ (equivalently } x_j \in x_i N).$$

8.7.1 Completeness

Once defined the concepts of Cauchy nets and convergent nets in profinite groups, it makes sense to ask whether they are equivalent or not, i.e. whether a profinite group is complete or not. This theorem is a positive answer to the question:

Theorem 8.7.5. *Every Cauchy net in a profinite group is convergent. We thus say that profinite groups are* complete*.*

Proof. Let G be a profinite group and $(x_i)_{i\in I}$ a Cauchy net. Define

$$X = \{x_i \mid i \in I\} \subseteq G.$$

Using Theorem 8.5.7, write $G \cong \varprojlim_{N\in\mathcal{N}} G/N$. Recall that the inverse system is given by $\{G/N, \pi_{NM}\}_{N,M\in\mathcal{N}}$ where $\pi_{NM}(xN) = xM$ for all $x \in G$ and $N \geq_{\mathcal{N}} M$ (i.e. $N \subseteq M$).

Since the net is Cauchy, for all $N \in \mathcal{N}$ there exists $i(N) \in \mathbb{N}$ such that for all $i, j \geq i(N)$, we have that $x_i N = x_j N$. With this notation, we will first prove that the tuple $(x_{i(N)}N)_{N\in\mathcal{N}}$ is coherent, that is, our goal is to show that $x_{i(N)}M = x_{i(M)}M$, for all $N \geq_{\mathcal{N}} M$. Since I is a directed set, let $i_0 \geq i(N), i(M)$. By the Cauchy condition, then we have $x_{i_0}M = x_{i(M)}M$ and $x_{i_0}N = x_{i(N)}N$, and the last equality implies $x_{i_0}M = x_{i(N)}M$ (because $N \subseteq M$). By the two previous equalities it follows that $x_{i(N)}M = x_{i(M)}M$ and hence $(x_{i(N)}N)_{N\in\mathcal{N}} \in \varprojlim_{N\in\mathcal{N}} G/N$.

Now we prove that the sequence is convergent. Let $x \in G$ correspond to the coherent sequence $(x_{i(N)}N)_{N\in\mathcal{N}}$, i.e.

$$(xN)_{N\in\mathcal{N}} = (x_{i(N)}N)_{N\in\mathcal{N}}$$

implying that for each $N \in \mathcal{N}$, we have $xN = x_{i(N)}N = x_i N$ for all $i \geq i(N)$; or, equivalently, $x_i \in xN$ for all $i \geq i(N)$. Thus the sequence $(x_i)_{i\in I}$ is convergent. $\square$

Now we are interested in discussing the existence of profinite completions of groups: we have already seen analogue results for metric spaces (Theorem 4.3.2) and fields with absolute values (Theorem 6.4.4).

Let G be a group. Choose a family $\mathcal{N}$ of normal subgroups with this property:

$$N, N' \in \mathcal{N} \implies \exists N'' \in \mathcal{N} \text{ such that } N'' \subseteq N \cap N'.$$

Clearly, $\mathcal{N}$ satisfies properties in Theorem 7.5.3 and so it defines a topology for which $\mathcal{N}$ is a fundamental system of neighborhoods of 1. Moreover, we shall require that all of them intersect at the identity, i.e. $\bigcap_{N \in \mathcal{N}} N = \{1\}$.

Examples 8.7.6. The following families of normal subgroups clearly satisfy the required properties:

(1) $G = (\mathbb{Z}, +)$ and $\mathcal{N} = \{p^n\mathbb{Z} \mid n \geq 0\}$;

(2) $G = (\mathbb{Z}, +)$ and $\mathcal{N} = \{n\mathbb{Z} \mid n \geq 1\}$.

The final result in these notes is the mentioned one about completions, which we state without proof.

Theorem 8.7.7. *In the situation above, the group*

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

is a profinite group in which G is dense.

The group $\hat{G}_{\mathcal{N}}$ of the previous theorem is called the *profinite completion* of G corresponding to the family $\mathcal{N}$.

For each $N \in \mathcal{N}$ let $\varphi_N : \hat{G}_{\mathcal{N}} \to G/N$ denote the projection homomorphisms, which turn out to be surjective. From Lemma 8.6.2 we obtain that $\{\ker \varphi_N\}_{N \in \mathcal{N}}$ is a fundamental system of neighborhoods of 1 consisting of open normal subgroups such that $\bigcap_{N \in \mathcal{N}} \ker \varphi_N = \{1\}$. By the First Isomorphism Theorem, we get that

$$\frac{\hat{G}_{\mathcal{N}}}{\ker \varphi_N} \cong \frac{G}{N}$$

for each $N \in \mathcal{N}$. There is an anology between the spaces G and $\hat{G}_{\mathcal{N}}$, shown in the following diagram:

$$\begin{tikzcd}
G \arrow[r, hook] \arrow[d, dash, "\unlhd"'] \arrow[dr, phantom, "\cong"] & \hat{G}_{\mathcal{N}} \arrow[d, dash, "\unlhd"] \\
N \arrow[r, dash] & \ker \varphi_N
\end{tikzcd}$$

Note that the family $\mathcal{N}$ defines the topology in G and the family $\{\ker \varphi_N\}_{N\in\mathcal{N}}$ defines the topology in $\hat{G}_N$.

There is one example of the previous isomorphism that we already know:

Example 8.7.8. Taking $G = \mathbb{Z}$ and $\mathcal{N} = \{p^n\mathbb{Z} \mid n \geq 0\}$, it turns out that $\hat{G}_{\mathcal{N}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$. Furthermore, by Lemma 6.6.1 we have $\ker \varphi_n = p^n\mathbb{Z}_p$ for all $n \in \mathbb{N}$, so

$$\frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p} \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}}.$$

There are two types of profinite completions which are extremely important. We present them in the following examples. First we need to restrict ourselves to a special type of group:

Definition 8.7.9. Let G be a group. We say that G is *residually finite* if the intersection of all its subgroups of finite index is trivial.

Examples 8.7.10. Let G be a residually finite group.

(1) Take the family

$$\mathcal{N} = \{N \trianglelefteq G \mid |G : N| < \infty\}.$$

Clearly it is a suitable family for a completion (note that it is residually finite and so $\bigcap_{N\in\mathcal{N}} N = \{1\}$). The profinite completion of G with respect to the family $\mathcal{N}$ is called the *profinite completion* of G, and it is simply denoted by $\hat{G}$.

In particular, when $G = \mathbb{Z}$, we have $\mathcal{N} = \{n\mathbb{Z} \mid n \in \mathbb{N}\}$ and the profinite completion is

$$\hat{\mathbb{Z}} = \varprojlim_{n\mathbb{Z}\in\mathcal{N}} \mathbb{Z}/n\mathbb{Z} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$$

where $\mathbb{N}$ is ordered by divisibility, see Examples 8.1.4 (3). We also have that

$$\hat{\mathbb{Z}} = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p).$$

However, we are not going to prove the last equality because it is much beyond the scope of this course.

(2) Let p be a prime number and define

$$\mathcal{N}_p = \{N \trianglelefteq G \mid |G : N| = p^n \text{ for some } n \geq 0\}.$$

Then the profinite completion with respect to the suitable family $\mathcal{N}_p$ is called the *pro-p completion* and it is simply denoted by $\hat{G}_p$. For all $N \in \mathcal{N}_p$, we have that $|G/N| = p^n$ and so G/N is a p-group. Hence, the pro-p completion

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

is a pro-p group.

Note that in the particular case $G = \mathbb{Z}$, the pro-p completion is the ring $\mathbb{Z}_p$ of p-adic numbers, i.e. $\hat{\mathbb{Z}}_p = \mathbb{Z}_p$.

Chapter 9

Solved exercises

Problem 12 (Exercise 23, [3]). Let K be a finite field. Show that the only absolute value on K is the trivial absolute value.

Solution. Let $|\ |$ be any absolute value on the finite field K. We shall analyze what the image is of each element in K.

(i) We know that $|0| = 0$ for any absolute value on K.

(ii) Consider $x \neq 0$ in K. As the field is finite we know that there exists $n \in \mathbb{N}$ such that $x^n = 1$. Actually, the multiplicative order of x is the smallest value for which the property hold, but the statement is also true choosing $n = |K^*| = |K| - 1$. Then:

$$x^n = 1 \implies |x|^n = |x^n| = |1| = 1 \implies |x| = 1$$

In the last implication notice that the absolute value of any element is a non-negative real number. Hence, the absolute value $|\ |$, is defined for any element in K, in the next way:

$$|x| = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0. \end{cases}$$

And by definition, this is the trivial absolute value. □

Problem 13 (Exercise 29, [3]). Let $\nu\colon K^* \to \mathbb{R}$ be a valuation. Show that the image of ν is an additive subgroup of $\mathbb{R}$. This is sometimes called the *value group* of the valuation ν. What is the value group of the p-adic valuation?

Solution. Since any valuation has the next property:

$$\nu(x \cdot y) = \nu(x) + \nu(y),$$

the valuation ν is a group homomorphism between the the groups $(K^*, \cdot)$ and $(\mathbb{R}, +)$. Then the image of the homomorphism, $\mathrm{im}\nu = \nu(K^*)$, is an additive subgroup of $\mathbb{R}$, as required.

Finally, in the particular case of the p-adic valuation in the field $\mathbb{Q}$, the valuation group is just $\mathbb{Z}$, i.e., $\nu(\mathbb{Q}^*) = \mathbb{Z}$. $\square$

Problem 14 (Exercise 38, [3])**.** The field $F(t)$ contains the subring of polynomials $F[t]$, but it also contains the subring $F[\frac{1}{t}]$ of "polynomials in $\frac{1}{t}$". In fact, every element of $F(t)$ can be written as a quotient of elements in $F[\frac{1}{t}]$, so this subring serves just as well as $F[t]$ as a starting point. Very well, in $F[\frac{1}{t}]$ the "polynomial" $\frac{1}{t}$ is clearly irreducible, so we can construct, as in Example 6.1.5, a $\frac{1}{t}$-adic valuation ν_1. Check that ν_1 is the same as the ν_∞ constructed above. This means that all the valuations we have constructed on $F(t)$ are of the "$p(t)$-adic" type.

Solution. Let $f \in F[t]$ and n be the unique number such that

$$f(t) = \left(\frac{1}{t}\right)^n g\left(\frac{1}{t}\right)$$

where $\frac{1}{t} \nmid g\left(\frac{1}{t}\right)$. Then

$$\nu_1(f(t)) = n.$$

On the other hand,

$$v_\infty(f(t)) = -\deg f.$$

Set $m = \deg f$. With this notation, the only thing we have to check is that $n = -m$. Write

$$f(t) = \lambda_0 + \lambda_1 t + \cdots + \lambda_m t^m$$

with $\lambda_m \neq 0$. Hence,

$$\begin{aligned} f(t) &= t^m \left(\lambda_0 \left(\frac{1}{t}\right)^m + \lambda_1 \left(\frac{1}{t}\right)^{m-1} + \cdots + \lambda_m\right) \\ &= \left(\frac{1}{t}\right)^{-m} \left(\lambda_0 \left(\frac{1}{t}\right)^m + \lambda_1 \left(\frac{1}{t}\right)^{m-1} + \cdots + \lambda_m\right) \end{aligned}$$

and since $\lambda_m \neq 0$, we have $\frac{1}{t} \nmid g\left(\frac{1}{t}\right)$. By uniqueness, it follows that $n = -m$ as we wanted to prove. $\square$

Problem 15 (Exercise 49, [3])**.** Let $K = \mathbb{Q}$ and $|\ | = |\ |_p$. Show that the closed ball $\overline{B}(0, 1)$ can be written as a disjoint union of open balls, as follows:

$$\overline{B}(0, 1) = B(0, 1) \cup B(1, 1) \cup B(2, 1) \cup \cdots \cup B(p - 1, 1).$$

This gives another proof that the closed unit ball is open, since unions of open sets are always open.

Solution. We must prove the equality and the disjointness. Disjointness.
We take two open balls of the right hand-side expression and prove that they are disjoint. As the p-adic absolute value is non-archimedean, by Proposition 6.1.13 two open balls are either disjoint or one is inside the other. In this case, as all the open balls have the same radius, $r = 1$, so if one is inside the other they necessarily are the same ball. Hence, the two open balls are either disjoint or the same ball.

Suppose by contradiction that two balls of the right-hand side expression are the same, i.e. $B(i, 1) = B(j, 1)$ for some $i, j \in \{0, \dots, p-1\}$. Then the center of one ball will be contained in the other ball, that is:

$$i \in B(j, 1) \implies |i - j|_p < 1.$$

On the other hand, $i - j$ is an integer number such that $-p < i - j < p$, which means that p does not divide $i - j$. Hence, $\nu_p(i - j) = 0$, so $|i - j|_p = p^{-\nu_p(i-j)} = 1$. This is a contradiction. Hence, all balls of the right-hand side expression are disjoint. Equality.
$\subseteq$) Let us see that for any $i \in \{1, \dots, p-1\}$, $\overline{B}(i, 1) = \overline{B}(0, 1)$.
Now, $\overline{B}(i, 1)$ and $\overline{B}(0, 1)$ are two closed balls with the same radius. Then as the p-adic absolute value is non-archimedean and according to Proposition 6.1.13 the two closed balls will be either the same ball or disjoint balls.
Furthermore, i is an integer number such that p does not divide i, because $i \in \{1, \dots, p-1\}$ and p is a prime number. So, $\nu_p(i) = 0$ and $|i|_p = p^{-\nu(i)} = 1$. Hence,

$$|i|_p = |i - 0|_p = 1 \implies i \in \overline{B}(0, 1).$$

Now, the two balls can not be disjoint so they must be the same closed ball. Then $B(i, 1) \subseteq \overline{B}(i, 1) = \overline{B}(0, 1)$ for all $i \in \{1, \dots, p-1\}$ and obviously $B(0, 1) \subseteq \overline{B}(0, 1)$. Finally,

$$\bigcup_{i=0}^{p-1} B(i, 1) \subseteq \overline{B}(0, 1).$$

$\supseteq$) Take any $z \in \overline{B}(0, 1)$.
Then $z = \frac{a}{b} \in \mathbb{Q}$ such that $|z|_p \leq 1$. Without loss of generality we can suppose that z is written in lowest terms as rational number. As we have seen in Example 6.2.5, if the absolute value of $\frac{a}{b}$ is less than or equal to one then $p \nmid b$, i.e., $\nu_p(b) = 0$.

We must find a value $k \in \{0, \dots, p-1\}$ such that $z \in B(k, 1)$, i.e.,

$$|z - k|_p = \left|\frac{a}{b} - k\right|_p = \left|\frac{a - kb}{b}\right|_p = p^{-\nu_p\left(\frac{a-kb}{b}\right)} < 1 \iff$$

$$\iff \nu_p\left(\frac{a - kb}{b}\right) > 0 \iff \nu_p(a - kb) > \nu_p(b) = 0 \iff p \mid a - kb.$$

We only must find a number $k \in \{0, \dots, p-1\}$ such that $p \mid a - kb$. Reducing modulo p, we need to find an element $\overline{k} \in \frac{\mathbb{Z}}{p\mathbb{Z}}$ such that $\overline{a - kb} = \overline{0}$. Then

$$\overline{a - kb} = \overline{0} \iff \overline{a} = \overline{kb} \iff \overline{k} = \overline{a}\overline{b}^{-1}.$$

Finally, notice that $p \nmid b$, i.e., $\gcd(b, p) = 1$, so the expression makes sense. Hence, there exists an integer $k \in \{0, \dots, p-1\}$ such that $z \in B(k, 1) \subseteq \bigcup_{i=0}^{p-1} B(i, 1)$. $\square$

Problem 16. Prove that any ultrametric space is totally disconnected

Solution. Assume by contradiction that there exists a connected subset, say C, such that $|C| > 1$. Let $x \neq y$ be two points in C. Since the points are distinct, by the Hausdorff property of metrizable spaces, there exist $r, s > 0$ such that $B(x, r) \cap B(y, s) = \varnothing$. By Proposition 6.1.13, $B(x, r)$ is clopen and so $B(x, r) \cap C$ is clopen in the subspace C. It is non-empty (x is in the intersection) and it is proper (because $y \in C$ but since $B(x, r) \cap B(y, s) = \varnothing$, it follows that $y \notin B(x, r)$). Hence, C is not connected, contradiction. $\square$

Problem 17. Let (X, τ) be a topological space. Define

$$\Delta(X) = \{(x, x) \mid x \in X\} \subseteq X \times X$$

Then the space (X, τ) is Hausdorff if and only if $\Delta(X)$ is closed in the product topology.

Solution. $\Rightarrow$) We shall see that $X \times X \setminus \Delta(X)$ is open. Let $(x, y) \in X \times X \setminus \Delta(X)$. Then , $x \neq y$. By hypothesis, there exist $U_x, U_y \in \tau$ such that $x \in U_x$, $y \in U_y$ and $U_x \cap U_y = \varnothing$. Now we prove that $U_x \times U_y \subseteq X \times X \setminus \Delta(X)$. Let $(z, t) \in U_x \times U_y$ and assume by way of contradiction that $(z, t) \notin X \times X \setminus \Delta(X)$, that is, $(z, t) \in \Delta(X)$, meaning that $z = t$, and so $z \in U_x \cap U_y$, contradicting our assumption. Finally notice that $U_x \times U_y \in \beta_{Tych}$, and so $X \times X \setminus \Delta(X)$ is open.

$\Leftarrow$) Let $x \neq y$ be two points in X. By definition of $\Delta(X)$, we have that $(x, y) \notin \Delta(X)$, i.e. $(x, y) \in X \times X \setminus \Delta(X)$ which is an open set in the product. Then there exists $U_x \times U_y \in \beta_{Tych}$ (with $U_x, U_y \in \tau$) such that $(x, y) \in U_x \times U_y \subseteq X \times X \setminus \Delta(X)$. If we prove that U_x and U_y are disjoint, the Hausdorff property will be proved. By contradiction, suppose that $z \in U_x \cap U_y$. Then $(z, z) \in U_x \times U_y \subseteq X \times X \setminus \Delta(X)$ and $(z, z) \in \Delta(X)$ at the same time, which is impossible. $\square$

Problem 18. Prove the First Isomorphism Theorem for topological groups.

Solution. Notice that $\ker f$ is a normal subgroup of G, so we have a topological group structure on the quotient. By the First Isomorphism Theorem for groups, φ is an isomorphism of groups. So if we prove that φ is continuous and open, we have finished. As usual, denote p the canonical projection of G onto $G/\ker f$. It is clear that $f = \varphi \circ p$.

$$\begin{tikzcd} G \arrow[d, "p"'] \arrow[dr, "f"] & \\ G/\ker f \arrow[r, "\varphi"'] & H \end{tikzcd}$$

By Lemma 7.4.2, since f is continuous, φ is continuous.

Now we check that φ is open. Let U be an open set in $G/\ker f$. We have to show that $\varphi(U)$ is open in H. p^{-1} is continuous, so $p^{-1}(U)$ is open in G. Furthermore, f is open, so $f(p^{-1}(U))$ is open in H. Taking into account that p is surjective and that the diagram above commutes, we obtain that

$$f(p^{-1}(U)) = (\varphi \circ p \circ p^{-1})(U) = \varphi(U)$$

and therefore $\varphi(U)$ is open.

□

Problem 19. Prove the Third Isomorphism Theorem for topological groups.

Solution. Define $f\colon G/N \to G/M$ such that $f(xN) = xM$. If we prove that the map f is open, continuous, surjective and a homomorphism of groups with $\ker f = M/N$, we have finished (by the First Isomorphism Theorem).

The map f is well-defined because

$$xN = yN \implies y^{-1}x \in N \subseteq M \implies xM = yM$$

and clearly it is a surjective group homomorphism and $\ker f = M/N$.

Now we prove that is is continuous. Take p the canonical projection from G onto G/M and q the canonical projection from G onto G/N. We have the following commutative diagram:

$$\begin{tikzcd} G \arrow[d, "q"'] \arrow[dr, "p"] & \\ G/N \arrow[r, "f"'] & G/M \end{tikzcd}$$

By Lemma 7.4.2, since p is continuous, f is continuous.

Finally, we will prove that f is open. Let U be an open subset in G/N. We have to see that $f(U)$ is open in G/M, or, equivalently, that $p^{-1}(f(U))$ is open in G. We have the following chain of equalities:

$$\begin{aligned} p^{-1}(f(U)) &= \{x \in G \mid xM = f(yN) \text{ for some } yN \in U\} \\ &= \{x \in G \mid xM = yM \text{ for some } y \in q^{-1}(U)\} \\ &= \{x \in G \mid x \in yM \text{ for some } y \in q^{-1}(U)\} \\ &= \bigcup_{y \in q^{-1}(U)} yM = q^{-1}(U)M = \bigcup_{x \in M} q^{-1}(U)x = \bigcup_{x \in M} r_x(q^{-1}(U)) \end{aligned}$$

Since all r_x are open and since q is continuous, all $r_x(q^{-1}(U))$ are open and so the union is open. $\square$

Problem 20. Let G be a topological group and let N be a normal subgroup of G. Then, G/N is Hausdorff if and only if N is closed.

Solution. Denote T a transversal set of G and p the natural projection to the quotient topological group.

$\Rightarrow$) Suppose G/N is T_2. Since the singletons are closed in G/N and p is continuous, $p^{-1}(\{p(t)\})$ is closed for each $t \in T$. In particular, $N = p^{-1}(\{p(1)\})$ is closed.

$\Leftarrow$) Suppose that N is closed in G, since G/N is a topological group it is enough proving that it is T_1. Since the translations are homeomorphisms all the cosets are closed. Moreover, for any $x \in G/N$ we can write $\{x\} = p(tN)$ for a $t \in T$. Finally, since the natural projection p is closed $\{x\} = p(tN)$ is closed, so all the singletons are closed. Therefore, G/N is Hausdorff. $\square$

Problem 21. Let G be a topological group and let H be a subgroup of G. Prove that $\overline{H}$ is a closed subgroup of G.

Solution. Clearly, $\overline{H}$ is closed and we shall see that it is a subgroup. Define the continuous function $f\colon G \times G \to G$ such that $f(x, y) = xy^{-1}$. Since $\overline{H}$ is closed in G and f is a continuous function, $f^{-1}(\overline{H})$ is a closed subset of $G \times G$. Futhermore, H is a subgroup, so

$$f(H \times H) \subseteq H \subseteq \overline{H} \implies H \times H \subseteq f^{-1}(\overline{H}) \implies \overline{H \times H} \subseteq \overline{f^{-1}(\overline{H})} = f^{-1}(\overline{H}).$$

Moreover, by Exercise 1, $\overline{H} \times \overline{H} = \overline{H \times H}$. Hence,

$$\overline{H} \times \overline{H} = \overline{H \times H} \subseteq f^{-1}(\overline{H}) \implies f(\overline{H} \times \overline{H}) \subseteq \overline{H}.$$

This means that for any $x, y \in \overline{H}$, $f(x, y) = xy^{-1} \in \overline{H}$ and so $\overline{H}$ is a subgroup of G. $\square$

Problem 22. Let G be a topological group, let X be an open subset and let Y be any subset of G. Prove that XY is open.

Solution. The right translation is a homeomorphism, so for each $y \in Y$, $l_y(X) = Xy$ is open. Furthermore

$$XY = \bigcup_{y \in Y} Xy.$$

Finally XY is the union of open subsets, so it is open. $\square$

Problem 23. Let G be a topological group, let X be a closed subset and let Y be any subset of G. Is XY closed? If Y is closed? And if Y is finite?

Solution. Generally the product set XY is not closed, even if the both subsets (X and Y) are closed. As a counter-example consider the topological group $(\mathbb{R}, \tau_u, +)$. Then, $X = \mathbb{Z}$ and $Y = \sqrt{2}\mathbb{Z}$ are both closed subsets in G, but $XY = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ is a proper dense subset of $\mathbb{R}$. Hence, $\overline{XY} \neq XY$ and so it is not closed.

However, the statement is true when Y is finite. As in the Problem 22 the right translation is a homeomorphism, so $l_y(X) = Xy$ is closed for each $y \in Y$. Moreover, since XY is the finite union of closed subsets ($XY = \bigcup_{y \in Y} Xy$), it is closed. $\square$

Problem 24. Any cartesian product of topological spaces is homeomorphic to an inverse limit. Moreover, if the factors are topological groups, we also have an isomorphism of topological groups. In particular, if the groups are finite with discrete topology, the cartesian product can be regarded as a profinite group.

Solution. Given an arbitrary index set I (not necessarily directed) and a family $\{(X_i, \tau_i)\}_{i \in I}$ of topological spaces, consider the cartesian product $X = \prod_{i \in I} X_i$ with Tychonoff topology. To simplify notation, we shall denote its elements (x_i) or (y_i), avoiding subindexes.

Consider the set $\mathcal{J} = \{F \subseteq I \mid F \text{ is finite}\}$, which is a directed set with the inclusion (see 8.1.2). For each $F \in \mathcal{J}$ define the finite cartesian product

$$X_F = \prod_{j \in F} X_j$$

with Tychonoff topology. Note that X_F can be seen as a subspace of $\prod_{i \in I} X_i$. For any $F, F' \in \mathcal{J}$ such that $F' \leq F$ (i.e. $F' \subseteq F$) we may consider the natural projection map $\varphi_{FF'} : X_F \to X_{F'}$. Naturally, $(X_F, \varphi_{FF'})_{F,F' \in \mathcal{J}}$ is an inverse system, and it turns out that

$$X \cong \varprojlim_{F \in \mathcal{J}} X_F.$$

In order to construct an homeomorphism we shall use the universal property of inverse limits.

$$\begin{tikzcd}
 & \varprojlim\limits_{F \in \mathcal{J}} X_F \arrow[dr, "\varphi_F"] & \\
X \arrow[ur, dashed, "\psi"] \arrow[rr, "\psi_F"] & & X_F
\end{tikzcd}$$

First, the natural projections $\psi_F \colon X \to X_F$ are clearly continuous and compatible with the connecting maps, so according to Proposition 8.1.7, they give rise to the continuous map

$$\begin{array}{cccc} \psi\colon & X & \to & \varprojlim_{F \in \mathcal{J}} X_F \\ & (x_i) & \mapsto & \Big(\psi_F\big((x_i)\big)\Big)_{F \in \mathcal{J}}. \end{array}$$

On the one hand, if $(x_i) \neq (y_i)$, then $x_j \neq y_j$ for some $j \in I$. Thus, for $F = \{j\} \in \mathcal{J}$ we have $\psi_F((x_i)) \neq \psi_F((y_i))$ and hence their image through ψ is also different. This shows that the map ψ is injective.

On the other hand, any coherent tuple $(x_F)_{F\in\mathcal{J}} \in \varprojlim_{F\in\mathcal{J}} X_F$ can be used to construct an element in X as follows: for each $i \in I$ choose $F_i \in \mathcal{J}$ containing it and let x_i be the ith coordinate of x_{F_i}. Point that it does not matter the set we choose, because if F' and F'' contain i then $F = F' \cup F'' \in \mathcal{J}$ also contains it, and by compatibility condition we have

$$\varphi_{FF'}(x_F) = x_{F'} \text{ and } \varphi_{FF''}(x_F) = x_{F''}.$$

Hence, the ith coordinate is the same in x_F, $x_{F'}$ and $x_{F''}$ and we can define the tuple (x_i) unambiguously. It is trivial to check that $\psi((x_i)) = (x_F)_{F\in\mathcal{J}}$, so it is also surjective.

Finally, let's show that ψ is an open map. Due to bijectivity it suffices to prove that the image of a basic subopen set of X is open in $\varprojlim_{F\in\mathcal{J}} X_F$. Following the notation of Chapter 1, for any $j \in I$ and $U_j \in \tau_j$ we have

$$\begin{aligned}\psi(\pi_j^{-1}(U_j)) &= \{\psi((x_i)) \in \varprojlim_{F\in\mathcal{J}} X_F \mid (x_i) \in \pi_j^{-1}(U_j)\} \\ &= \{\psi((x_i)) \in \varprojlim_{F\in\mathcal{J}} X_F \mid x_j \in U_j\} \\ &= \{(x_F)_{F\in\mathcal{J}} \in \varprojlim_{F\in\mathcal{J}} X_F \mid \text{The } j\text{th coordinate of } x_F \text{ belongs to } U_j\}.\end{aligned}$$

Let us see that it is exactly the set $\pi_{\{j\}}^{-1}(U_j) \cap \varprojlim_{F\in\mathcal{J}} X_F$, clearly open. Note that this time the projection is considered in the cartesian product $\prod_{F\in\mathcal{J}} X_F$ and the space $X_{\{j\}} = X_j$, so the definition makes sense. One inclusion is straightforward, so let $(x_F)_{F\in\mathcal{J}} \in \pi_{\{j\}}^{-1}(U_j) \cap \varprojlim_{F\in\mathcal{J}} X_F$. We must show that whenever $j \in F$, the jth coordinate of x_F is in U_j. Point that under these assumptions $x_{\{j\}} = x_j \in U_j$. Then by compatibility condition we have

$$\varphi_{F\{j\}}(x_F) = x_{\{j\}} = x_j,$$

so the jth coordinate of x_F is in U_j, as desired.

For the second part, assume that the factors are topological groups. Naturally, the sets X_F are also topological groups with the operation componentwise. Furthermore, the connecting maps used before, the natural projections, are clearly group homomorphisms (and so happens with the projections ψ_F). Therefore, $\varprojlim_{F\in\mathcal{J}} X_F$ is a subgroup of the corresponding cartesian product, so we only have to show that the map ψ defined before is also a group homomorphism. We have

$$\begin{aligned}\psi((x_i \cdot y_i)) &= \Big(\psi_F\big((x_i \cdot y_i)\big)\Big)_{F\in\mathcal{J}} \\ &= \Big(\psi_F\big((x_i)\big) \cdot \psi_F\big((y_i)\big)\Big)_{F\in\mathcal{J}} \\ &= \Big(\psi_F\big((x_i)\big)\Big)_{F\in\mathcal{J}} \cdot \Big(\psi_F\big((y_i)\big)\Big)_{F\in\mathcal{J}} = \psi\big((x_i)\big) \cdot \psi\big((y_i)\big),\end{aligned}$$

so ψ is also a group homomorphism.

For the last part, point that if the groups X_i are finite, so are the finite products X_F. Moreover, if the topology of each X_i is the discrete, so is the topology of X_F, because in the finite case the product topology coincides with the box topology. Therefore, we have an isomorphism of topological groups between the cartesian product and an inverse limit of finite groups with discrete topology, i.e., a profinite group. □

Problem 25. Let $(X_i, \varphi_{i,j})_{i,j\in I}$ be an inverse system of compact and Hausdorff topological spaces, Y another compact and Hausdorff topological space and $\{\psi_i \colon Y \to X_i\}_{i\in I}$ a family of continuous maps compatible with the inverse system. If ψ_i is surjective for all $i \in I$ then the continuous map ψ given by the universal property is also surjective (see Proposition 8.1.7).

Solution. Recall that we saw in Examples 8.3.4 (1) that any topological space can be regarded as an inverse limit just taking any directed set and the identity as connecting maps. In this case it will be convenient to work with $\varprojlim_{i\in I} Y$ rather than with Y itself. Let $(x_i)_{i\in I} \in \varprojlim_{i\in I} X_i$ and define the sets $Y_i = \psi_i^{-1}(\{x_i\})$. Due to surjectivity they are nonempty and since X_i is Hausdorff singletons are closed there, so Y_i is also closed. Moreover, Y_i is a closed subspace of a compact space, so it is also compact and, of course, Hausdorff (that property is inherited by any subspace).

In order to show that $(Y_i, \mathrm{id}_{ij|Y_i})_{i,j\in I}$ is an inverse system we only have to check that for $i \geq j$ we have $\mathrm{id}_{ij}(Y_i) = Y_i \subseteq Y_j$, because the definition axioms follow from the fact that we are just taking subsets and restrictions of an inverse system. By the compatibility we have $\varphi_{ij} \circ \psi_i = \psi_j$, so for any $y \in Y_i$ we have

$$\psi_j(y) = \varphi_{ij}(\psi_i(y)) = \varphi_{ij}(x_i) = x_j \implies y \in \psi_j^{-1}(\{x_j\}) = Y_j.$$

Therefore we can consider $\varprojlim_{i\in I} Y_i$, which is clearly a subset of $\varprojlim_{i\in I} Y$. Furthermore, by Theorem 8.3.5 it is nonempty, which means that there exists $(y)_{i\in I} \in \varprojlim_{i\in I} Y$ with $y \in \psi_i^{-1}(\{x_i\})$ for all $i \in I$. Thus $\psi(y) = (\psi_i(y))_{i\in I} = (x_i)_{i\in I}$ and the map is surjective. □

Problem 26. Let G be a profinite group. Prove that G/N is a profinite group if and only if N is normal and closed in G.

Solution. At first, notice that so that the quotient makes sense N must be normal.

In order to prove the *only if* implication; being G/N a profinite group means that G/N is T_2, and according to Exercise 20, N is closed in G.

To deal with *if*, since N is closed according to the above exercise G/N is Hausdorff. Furthermore, the quotient group G/N is also totally disconnected; because it is a closed subgroup of a totally disconnected group (Lemma 8.5.10). In fact, by Lemma 8.6.2 there exists some i such that $V_i = \ker \varphi_i \leq N$ and V_i is a neighborhood of the identity. Therefore, G/N is a subgroup of G/V_i, which is totally disconnected by Corollary 7.3.2.

Finally, consider the canonical epimorphism $\pi_N \colon G \to G/N$ which is continuous and onto. Moreover, G is compact (since it is a profinite group), so $\pi_N(G) = G/N$ is compact. Therefore, G/N is a compact, T_2 and totally disconnected topological space, so by Theorem 8.5.7 it is a profinite group. □

Problem 27. Prove that

$$SL_2(\mathbb{Z}_p) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z}_p,\ \det A = 1 \right\}$$

is a profinite group.

Solution. We have that $SL_2(\mathbb{Z}_p) \subseteq \mathcal{M}_2(\mathbb{Z}_p)$ and clearly $\mathcal{M}_2(\mathbb{Z}_p)$ is homeomorphic to $\mathbb{Z}_p^4$ (note that since both sets are bijective, we can give $\mathcal{M}_2(\mathbb{Z}_p)$ the topology that turns this bijection into a homeomorphism). Now $\mathbb{Z}_p^4$ is compact, Hausdorff and totally disconnected and these properties are topological so $\mathcal{M}_2(\mathbb{Z}_p)$ is also provided with them. Besides, being Hausdorff and totally disconnected are hereditary properties, hence $SL_2(\mathbb{Z}_p)$ satisfies them.

Moreover, the determinant map $\det \colon \mathcal{M}_2(\mathbb{Z}_p) \to \mathbb{Z}_p$ is continuous because it is a combination of sums and products in $\mathbb{Z}_p$ and $\{1\}$ is a closed set in $\mathbb{Z}_p$ (notice that $\mathbb{Z}_p$ is totally disconnected). Thus, $\det^{-1}(\{1\}) = SL_2(\mathbb{Z}_p)$ is closed in $\mathcal{M}_2(\mathbb{Z}_p)$. Now, applying Proposition 8.0.2, we conclude that $SL_2(\mathbb{Z}_p)$ is compact. Therefore we have proved that $SL_2(\mathbb{Z}_p)$ satisfies (ii) in Theorem 8.5.7, so it is a profinite group. □

Bibliography

[1] N. Bourbaki, *Elements of mathematics, General Topology, Chapters 1-4*, second edition, Springer-Verlag, 1995.

[2] J. Duoandikoetxea, *Espazio Metrikoen Topologia*, Udako Euskal Unibertsitatea, 1982.

[3] F. Q. Gouvêa, *p-adic Numbers, An Introduction*, second edition, Springer-Verlag, 1997.

[4] J. R. Munkres, *Topology*, second edition, Prentice Hall, 2000.

[5] L. Ribes, P. Zalesskii, *Profinite Groups*, second edition, Springer-Verlag, 2010.

[6] S. Willard, *General Topology*, Dover edition, Dover Publications, 2004.