# The Pontryagin duals of $\mathbf{Q}/\mathbf{Z}$ and $\mathbf{Q}$

Jordan Bell

January 5, 2015

## 1 Pontryagin duality

Write $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. A **character** of a locally compact abelian group $G$ is a continuous group homomorphism $G \to S^1$. We denote by $\widehat{G}$ the set of characters of $G$, where for $\phi_1, \phi_2 \in \widehat{G}$ and $x \in G$, we define $(\phi_1\phi_2)(x) = \phi_1(x)\phi_2(x)$. We assign $\widehat{G}$ the final topology for the family of functions $\{\phi \mapsto \phi(x) : x \in G\}$, i.e., the coarsest topology on $\widehat{G}$ so that for each $x \in G$, the function $\phi \mapsto \phi(x)$ is continuous $\widehat{G} \to S^1$. With this topology, it is a fact that $\widehat{G}$ is itself a locally compact abelian group, called the **Pontryagin dual of** $G$. It is a fact that the Pontryagin dual of a discrete abelian group is compact and that the Pontryagin dual of compact abelian group is discrete.[1] The **Pontryagin duality theorem** states that in the category of locally compact abelian groups, there is a natural isomorphism from the double dual functor to the identity functor.[2]

With the subspace topology inherited from $\mathbb{R}$, one checks that a compact subset of $\mathbb{Q}$ has empty interior, and therefore $\mathbb{Q}$ is not locally compact. Thus, to work with the rational numbers in the category of locally compact abelian groups, we cannot use the subspace topology inherited from $\mathbb{R}$. Rather, we assign $\mathbb{Q}$ the discrete topology. (Any abelian group is a locally compact abelian group when assigned the discrete topology.) From now on, when we speak about $\mathbb{Q}$, unless we say otherwise it has the discrete topology.

Because we use the discrete topology with $\mathbb{Q}$, its Pontryagin dual $\widehat{\mathbb{Q}}$ is a compact abelian group, which we wish to describe in a tractable way.

## 2 The $p$-adic integers

For a prime $p$ and for $n \geq 1$, $\mathbb{Z}/p^n$ with the discrete topology is a compact abelian group. For $n \geq m$, let $\pi_{n,m} : \mathbb{Z}/p^n \to \mathbb{Z}/p^m$ be the projection map. The compact abelian groups $\mathbb{Z}/p^n$ and the continuous group homomorphisms $\pi_{n,m}$ are an inverse system in the category of locally compact abelian groups.

[1] Markus Stroppel, *Locally Compact Groups*, p. 175, Theorem 20.6.
[2] Markus Stroppel, *Locally Compact Groups*, p. 193, Theorem 22.6.

The inverse limit is a compact abelian group denoted by $\mathbb{Z}_p$, called the **$p$-adic integers**.

# 3 Q/Z and its Pontryagin dual

Let $G$ be an abelian group. The the **torsion subgroup** $T_G$ of $G$ is the collection of those elements of $G$ with finite order. We say that $G$ is a **torsion group** if $T_G = G$. Said differently, for $n$ a nonnegative integer, let $G[n]$ be the set of those $x \in G$ such that $nx = 0$. For $m|n$, let $i_{m,n} : G[m] \to G[n]$ be the inclusion map; indeed, if $x \in G[m]$ then

$$nx = \frac{n}{m} \cdot mx = \frac{m}{n} \cdot 0 = 0.$$

The groups $G[n]$ and the group homomorphisms are a direct system in the category of abelian groups, whose direct limit one checks is isomorphic to $T_G$.

For $p$ prime, the **$p$-primary subgroup** $G_p$ of $G$ is the set of those $x \in G$ such that for some $n \geq 1$, $x \in G[p^n]$. We can also express $G_p$ in the following way. For $m \leq n$, let $\iota_{m,n} : G[p^m] \to G[p^n]$ be the inclusion map; indeed, for $x \in G[p^m]$,

$$p^n x = p^{n-m} p^m x = p^{n-m} \cdot 0 = 0.$$

The groups $G[p^n]$ and the group homomorphisms $\iota_{m,n}$ are a direct system in the category of abelian groups, and one checks that the direct limit is isomorphic to $G_p$.

Let $x \in T_G$ and call its order $m$. Write $m = p_1^{e_1} \cdots p_r^{e_r}$ and put $m_i = \frac{m}{p_i^{e_i}}$. Then $\gcd(m_1, \ldots, m_r) = 1$, so there are integers $l_1, \ldots, l_r$ such that

$$l_1 m_1 + \cdots + l_r m_r = 1.$$

Thus

$$x = \left( \sum_{i=1}^{r} l_i m_i \right) x = \sum_{i=1}^{r} l_i (m_i x) = \sum_{i=1}^{r} l_i x_i,$$

where $x_i = m_i x$. Because $x_i$ has order $\frac{m}{m_i} = p_i^{e_i}$, it belongs to $G_{p_i}$ and so $l_i x_i \in G_{p_i}$, showing that every element of $T_G$ is a finite sum of elements of the $p$-primary components of $G$. Furthermore, one proves that if $x_p \in G_p$ and $y_p \in G_p$, with only finitely many $x_p, y_p$ nonzero, then $\sum_p x_p = \sum_p y_p$ implies that $x_p = y_p$ for each $p$. Therefore, $T_G$ is isomorphic to the direct sum

$$\bigoplus_p G_p.$$

The statement that $T_G$ is isomorphic to the direct sum of the $p$-primary components of $G$ is called the **primary decomposition theorem**.[3]

[3] Derek Robinson, *A Course in the Theory of Groups*, second ed., p. 94, Theorem 4.1.1.

It is straightforward to check that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of the abelian group $\mathbb{R}/\mathbb{Z}$. It can thus be modeled as the group of roots of unity in $S^1$. Writing $G = \mathbb{Q}/\mathbb{Z}$, for $p$ prime and for $n \geq 1$ it is apparent that $G[p^n]$ is isomorphic to the subgroup $\{\exp(2\pi im/p^n) : 0 \leq m < p^n - 1\}$ of $S^1$, and thus to $\mathbb{Z}/p^n$. Define $\iota_{m,n} : \mathbb{Z}/p^m \to \mathbb{Z}/p^n$, $m \leq n$, by $\iota_{m,n}(x) = p^{n-m}x$. The groups $\mathbb{Z}/p^n$ and the group homomorphisms $\iota_{m,n}$ are a direct system in the category of abelian groups, whose direct limit is denoted by $\mathbb{Z}(p^\infty)$, called the **Prüfer $p$-group**. Thus, the $p$-primary component of $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the Prüfer $p$-group $\mathbb{Z}(p^\infty)$. Now applying the primary decomposition theorem, we get that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the direct sum of all the Prüfer $p$-groups:

$$\mathbb{Q}/\mathbb{Z} \cong \bigoplus_p \mathbb{Z}(p^\infty). \tag{1}$$

We assign $\mathbb{Q}/\mathbb{Z}$ the discrete topology; indeed, the direct sum of discrete abelian groups is a discrete abelian group.

It is a fact that the Pontryagin dual of a direct sum of discrete abelian groups is isomorphic to the direct product of the Pontryagin duals of the summands. Also, we take as known that the Pontryagin dual of the compact abelian group $\mathbb{Z}_p$ is the discrete abelian group $\mathbb{Z}(p^\infty)$:

$$\widehat{\mathbb{Z}_p} \cong \mathbb{Z}(p^\infty).$$

Thus, in the category of locally compact abelian groups,

$$\widehat{\mathbb{Q}/\mathbb{Z}} \cong \prod_p \mathbb{Z}_p.$$

On the other hand, we stated above that if $G$ is an abelian group then $T_G$ is isomorphic to the direct limit of the direct system of groups $G[n]$ and inclusion maps $i_{m,n} : G[m] \to G[n]$ for $m|n$. Thus, $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the direct limit of the direct system of groups $\mathbb{Z}/n$ and maps $i_{m,n} : \mathbb{Z}/m \to \mathbb{Z}/n$ for $m|n$, $i_{m,n}(x) = \frac{n}{m} \cdot x$. The dual of the discrete abelian group $\mathbb{Z}/n$ is isomorphic to the compact abelian group $\mathbb{Z}/n$, and the dual of the map $i_{m,n} : \mathbb{Z}/m \to \mathbb{Z}/n$, for $m|n$, is the projection map $\pi_{n,m} : \mathbb{Z}/n \to \mathbb{Z}/m$. The dual of the direct system of groups $\mathbb{Z}/n$ and maps $i_{m,n}$ is the inverse system of groups $\mathbb{Z}/n$ and maps $\pi_{n,m}$, whose limit is a compact abelian group $\mathbb{Z}^\wedge$ called the **profinite completion of the integers**. It follows that

$$\widehat{\mathbb{Q}/\mathbb{Z}} \cong \mathbb{Z}^\wedge$$

as locally compact abelian groups, and thus also that

$$\prod_p \mathbb{Z}_p \cong \mathbb{Z}^\wedge$$

as locally compact abelian groups.

# 4 The $p$-adic integers

In this section we give a construction of the ring $\mathbb{Z}_p$. We have already defined $\mathbb{Z}_p$ as an inverse limit of compact abelian groups, and it can be proved that the additive group of the ring we construct here is indeed isomorphic as an abelian group to this inverse limit.[4] (In this section we do not assign a topology to our construction of $\mathbb{Z}_p$.) Our presentation in this section follows Robert.[5]

We start by defining objects, then put a group operation on the set of these objects.[6] Let $p$ be prime. A **$p$-adic integer** is a formal series of the form

$$\sum_{i\geq 0} a_i p^i, \qquad 0 \leq a_i \leq p_i - 1.$$

We denote the set of $p$-adic integers by $\mathbb{Z}_p$. As sets,

$$\mathbb{Z}_p = \prod_{i\geq 0} \{0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}^{\mathbb{Z}_{\geq 0}}.$$

For $a = \sum_{i\geq 0} a_i p^i, b = \sum_{i\geq 0} b_i p^i \in \mathbb{Z}_p$, we define $c = a + b$ inductively as follows. Define $\epsilon_0 = 0$ and define

$$c_0 = \begin{cases} a_0 + b_0 & a_0 + b_0 \leq p-1 \\ a_0 + b_0 - p & a_0 + b_0 > p-1. \end{cases}$$

Suppose that $c_n$ and $\epsilon_n$ have been defined. Now define

$$\epsilon_{n+1} = \begin{cases} 0 & a_n + b_n \leq p-1 \\ 1 & a_n + b_n > p-1, \end{cases}$$

and

$$c_{n+1} = \begin{cases} a_{n+1} + b_{n+1} + \epsilon_{n+1} & a_{n+1} + b_{n+1} + \epsilon_{n+1} \leq p-1 \\ a_{n+1} + b_{n+1} + \epsilon_{n+1} - p & a_{n+1} + b_{n+1} + \epsilon_{n+1} > p-1. \end{cases}$$

For example, let $a = 1p^0 + 0p + 0p^2 + \cdots$ and $b = (p-1)p^0 + (p-1)p + (p-1)p^2 + \cdots$, and put $c = a + b$. Then, $\epsilon_0 = 0$ and $c_0 = a_0 + b_0 - p = 0$. Next, $\epsilon_1 = 1$, with which $a_1 + b_1 + \epsilon_1 = 0 + (p-1) + 1 = p > p-1$, so $c_1 = p - p = 0$. Inductively, for any $n \geq 1$ we get that $\epsilon_n = 1$ and $c_n = 0$. Thus

$$a + b = 0p^0 + 0p^1 + 0p^2 + \cdots .$$

[4] See Alain M. Robert, *A Course in p-adic Analysis*, p. 33, §4.7.

[5] Alain M. Robert, *A Course in p-adic Analysis*, Chapter 1.

[6] Although constructing $p$-adic integers as formal series is concrete, one must then be cautious lest one does things with these series that seem reasonable because of experience working with series but that are not yet justified; defining $p$-adic integers as a completion of a metric space or as an inverse limit gives one abstract objects about which one only knows universal properties, and thus is not susceptible to making moves that are not permitted.

For $a = \sum_{i\geq 0} a_i p^i \in \mathbb{Z}_p$, define

$$\sigma(a) = \sum_{i\geq 0} (p-1-a_i)p^i.$$

We check that this satisfies $a + \sigma(a) + 1 = 0$, where $1 \in \mathbb{Z}_p$ means $1p^0 + 0p + 0p^2 + \cdots$. Thus, $1 + \sigma(a)$ is the additive inverse of $a$, i.e.,

$$-a = 1 + \sigma(a).$$

With addition thus defined, $\mathbb{Z}_p$ is an abelian group, with identity $0 = 0p^0 + 0p + 0p^2 + \cdots$. We define $\iota : \mathbb{Z} \to \mathbb{Z}_p$ as follows. For $n \in \mathbb{Z}_{\geq 0}$, there are unique $0 \leq a_i \leq p-1$, all but finitely many 0, such that $n = \sum_{i\geq 0} a_i p^i$; this is a finite sum of nonnegative integers because all but finitely many of the $a_i$ are 0. We define $\iota(n) \in \mathbb{Z}_p$ to be the formal series $\sum_{i\geq 0} a_i p^i$. On the other hand, for $a = \sum_{i\geq 0} a_i p^i \in \mathbb{Z}_p$ with all but finitely many of the $a_i$ equal to 0, we have $\sum_{i\geq 0} a_i p^i \in \mathbb{Z}_{\geq 0}$ and $\iota(\sum_{i\geq 0} a_i p^i) = a$. For $n \in \mathbb{Z}_{<0}$, we define

$$\iota(n) = -\iota(-n) = 1 + \sigma(\iota(-n)).$$

$\iota : \mathbb{Z} \to \mathbb{Z}_p$ is a group homomorphism.

For example, take $n = -4$ and $p = 3$. Then $\iota(-n) = \iota(4) = 1 \cdot 3^0 + 1 \cdot 3^1 + 0 \cdot 3^2 + \cdots$, so $\sigma(\iota(4)) = 1 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 + \cdots$. Then

$$\begin{aligned}\iota(-4) &= (1 \cdot 3^0 + 0 \cdot 3^1 + 0 \cdot 3^2 + \cdots) + (1 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 + \cdots) \\ &= 2 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \cdots\end{aligned}$$

Multiplication of $p$-adic integers is defined similarly to addition of $p$-adic integers.[7] For example, take $p = 5$ and let $a = \iota(2 \cdot 5^0 + 2 \cdot 5^1 + 3 \cdot 5^2)$ $b = \iota(3 \cdot 5^0 + 4 \cdot 5^1)$. Then,

$$a \cdot b = \iota(1 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4).$$

For any prime $p$, $\iota(1) = 1p^0 + 0p^1 + 0p^2 + \cdots$ and so

$$\begin{aligned}\iota(-1) &= 1 + \sigma(\iota(1)) \\ &= (1p^0 + 0p^1 + 0p^2 + \cdots) + ((p-2)p^0 + (p-1)p^1 + (p-1)p^2 + \cdots) \\ &= (p-1)p^0 + (p-1)p^1 + (p-1)p^2 + \cdots \\ &= (p-1)\sum_{i\geq 0} p^i.\end{aligned}$$

One then checks that

$$\iota(1) = (1-p)\sum_{i\geq 0} p^i.$$

[7] That it is cumbersome to define multiplication of elements of $\mathbb{Z}_p$ shows that defining $p$-adic integers as formal series invites sloppiness; one merely assumes that everything works out like one wants it to.

Thus, the multiplicative inverse of $1-p$ in $\mathbb{Z}_p$ is $\sum_{i\geq 0} p^i$.

We define the **$p$-adic valuation** $v_p : \mathbb{Z}_p \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by $v_p(0) = \infty$ and defining $v_p(a)$ to be the least $i$ such that $a_i \neq 0$. For example,

$$v_p(0 \cdot p^0 + 0 \cdot p^1 + 3 \cdot p^2 + \cdots) = 2.$$

If $a, b \in \mathbb{Z}_p$ are each nonzero, then for $c = a \cdot b$ we have $0 \leq c_{v_p(a)+v_p(b)} \leq p-1$ and

$$c_{v_p(a)+v_p(b)} \equiv a_{v_p(a)} b_{v_p(b)} \pmod{p}$$

and because $p \nmid a_{v_p(a)}$ and $p \nmid b_{v_p(b)}$, we have that $c_{v_p(a)+v_p(b)} \neq 0$. It follows that

$$v_p(a \cdot b) = v_p(a) + v_p(b).$$

In particular, this shows that $\mathbb{Z}_p$ is an integral domain.

# 5 Reduction modulo $p$, maximal ideals, and local rings

Define $\epsilon : \mathbb{Z}_p \to \mathbb{Z}/p$ by

$$\epsilon\left(\sum_{i\geq 0} a_i p^i\right) = a_0 + (p).$$

This is a homomorphism of unital rings called **reduction modulo** $p$. We have

$$\ker \epsilon = \left\{ \sum_{i\geq 0} a_i p^i \in \mathbb{Z}_p : a_0 = 0 \right\} = p\mathbb{Z}_p.$$

Because $\epsilon$ is a surjective homomorphism of unital rings and $\mathbb{Z}/p$ is a field, $\ker \epsilon$ is a maximal ideal in the ring $\mathbb{Z}_p$. Denote by $\mathbb{Z}_p^*$ the set of invertible elements of $\mathbb{Z}_p$. It can be proved[8] that

$$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p.$$

Because the set of noninvertible elements in $\mathbb{Z}_p$ is a proper ideal, $\mathbb{Z}_p$ is a **local ring**, and hence the maximal ideal $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$. For any nonzero $a \in \mathbb{Z}_p$, it is immediate that $p^{-v_p(a)} a \in \mathbb{Z}_p^*$; in other words, for any nonzero $a \in \mathbb{Z}_p$, there is some $u \in \mathbb{Z}_p^*$ such that $a = p^{v_p(a)} u$.

We now prove that $\mathbb{Z}_p$ is a principal ideal domain.[9]

**Theorem 1.** *The ideals in $\mathbb{Z}_p$ are $\{0\}$ and $(p^k) = p^k\mathbb{Z}_p$, $k \in \mathbb{Z}_{\geq 0}$.*

[8] Alain M. Robert, *A Course in p-adic Analysis*, p. 5, §1.5.
[9] Alain M. Robert, *A Course in p-adic Analysis*, p. 6, §1.6.

*Proof.* It is straightforward to check that indeed these are ideals in $\mathbb{Z}_p$. Suppose that $I \neq \{0\}$ is an ideal in $\mathbb{Z}_p$. Since $I \neq \{0\}$, there is some element $a \in I$ such that

$$v_p(a) = \min\{v_p(x) : x \in I\}.$$

Let $k = v_p(a)$. Then $u = p^{-k}a \in \mathbb{Z}_p^*$, i.e., $p^k = u^{-1}a$. Since $a \in I$ and $I$ is an ideal, this shows that $p^k \in I$. This shows that $p^k\mathbb{Z}_p \subset I$. On the other hand, let $b \in I$ and write $l = v_p(b)$. There is some $u' \in \mathbb{Z}_p^*$ such that $b = p^l u'$, and then $b = p^k p^{l-k} u'$. But $l - k \geq 0$ so $p^{l-k}u' \in \mathbb{Z}_p$, hence $b \in p^k\mathbb{Z}_p$. This shows that $I \subset p^k\mathbb{Z}_p$, completing the proof. □

# 6 Topology of the *p*-adic integers

As sets,

$$\mathbb{Z}_p = \prod_{i \geq 0} \{0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}^{\mathbb{Z}_{\geq 0}}.$$

We assign $\mathbb{Z}_p$ the product topology, with which it is a compact and metrizable topological space. (It is compact because the set $\{0, 1, \ldots, p-1\}$ with the discrete topology is compact, and it is metrizable because it is a countable product and $\{0, 1, \ldots, p-1\}$ is metrizable with the discrete metric.) One checks that the product topology on $\mathbb{Z}_p$ is induced by the **$p$-adic metric** $d_p$ defined by

$$d_p(a, b) = p^{-v_p(a-b)}.$$

The map $a \mapsto pa$ satisfies

$$d_p(pa, pb) = p^{-v_p(pa-pb)} = p^{-v_p(a-b)-1} = \frac{1}{p} d_p(a, b),$$

which shows that $a \mapsto pa$ is continuous $\mathbb{Z}_p \to \mathbb{Z}_p$.

We say that a group $G$ with a topology is a **topological group** if its topology is Hausdorff, if $(x, y) \mapsto x + y$ is continuous $G \times G \to G$, and if $x \mapsto -x$ is continuous $G \to G$. Because $\mathbb{Z}_p$ is metrizable it is Hausdorff, and we now prove that the group operations are continuous using its topology.

**Theorem 2.** *$(x, y) \mapsto x + y$ is continuous $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ and $x \mapsto -x$ is continuous $\mathbb{Z}_p \to \mathbb{Z}_p$.*

*Proof.* The product topology on $\mathbb{Z}_p \times \mathbb{Z}_p$ is induced by the metric $\rho((x, y), (a, b)) = d_p(x, a) + d_p(y, b)$. Let $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$. If $\rho((x, y), (a, b)) \leq p^{-n}$, then $p^{-v_p(x-a)} = d_p(x, a) \leq p^{-n}$, hence $v_p(x-a) \geq n$, and likewise $v_p(y-b) \geq n$. But $v_p(w + z) \geq \min\{v_p(w), v_p(z)\}$ and $v_p(-w) = v_p(w)$, so $v_p(x - a - (y - b)) \geq n$. Thus

$$d_p(x - a, y - b) = p^{-v_p(x-a-(y-b))} \leq p^{-n}.$$

This shows that $(x, y) \mapsto x - y$ is continuous at $(a, b)$, and since $(a, b)$ was arbitrary, $(x, y) \mapsto x - y$ is continuous $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$, showing that $\mathbb{Z}_p$ is a topological group. □

To prove that the multiplicative group $\mathbb{Z}_p^*$ is a topological group we use the following lemma. We remind ourselves that if $X$ is a topological space and $x \in X$, a **neighborhood of** $x$ is a subset $N$ of $X$ for which there is an open subset satisfying $x \in U \subset N$. The collection of all neighborhoods of a point $x$ is called the **neighborhood filter at** $x$. A **neighborhood base at** $x$ is a collection $\mathscr{B}$ of neighborhoods of $x$ such that if $N$ is a neighborhood of $x$ then there is some $B \in \mathscr{B}$ such that $B \subset N$; namely, a neighborhood base at $x$ is a filter base for the neighborhood filter at $x$.

**Lemma 3.** *The collection* $\{1 + p^n\mathbb{Z}_p : n \in \mathbb{Z}_{>0}\}$ *is a neighborhood base at* 1.

$\mathbb{Z}_p^*$ is metrizable with the $p$-adic metric, so it is Hausdorff. Using the above lemma, we can now prove that $\mathbb{Z}_p^*$ is a topological group, and then that $\mathbb{Z}_p$ is a topological ring.[10]

**Theorem 4.** $(x, y) \mapsto x \cdot y$ *is continuous* $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ *and* $x \mapsto x^{-1}$ *is continuous* $\mathbb{Z}_p^* \to \mathbb{Z}_p^*$.

*Proof.* Let $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ and suppose that $x \in a + p^n\mathbb{Z}_p$ and $y \in b + p^n\mathbb{Z}_p$. Thus, there are $\alpha, \beta \in \mathbb{Z}_p$ such that $x = a + p^n\alpha$ and $y = b + p^n\beta$. Then

$$x \cdot y = a \cdot b + p^n(a + b + p^n\alpha \cdot \beta) \in a \cdot b + p^n\mathbb{Z}_p.$$

This shows that $(x, y) \mapsto x \cdot y$ is continuous at $(a, b)$, and therefore that $(x, y) \mapsto x \cdot y$ is continuous $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$.

Let $a \in \mathbb{Z}_p^*$ and suppose that $x \in a + p^n\mathbb{Z}_p$. There is some $\alpha \in \mathbb{Z}_p$ such that $x = a(1 + p^n\alpha)$, and then there is some $\beta \in \mathbb{Z}_p$ such that

$$(1 + p^n\alpha)^{-1} = \sum_{i \geq 0} (-p^n\alpha)^i = 1 + p^n\beta.$$

Then

$$x^{-1} = a^{-1}(1 + p^n\beta) \in a^{-1} + p^n\mathbb{Z}_p.$$

This shows that $x \mapsto x^{-1}$ is continuous at $a$, and therefore that it is continuous $\mathbb{Z}_p^* \to \mathbb{Z}_p^*$. □

# 7 Rings of fractions and localization

Let $R$ be an integral domain with unity 1. A subset $S$ of $R$ is said to be a **multiplicative set** if $0 \notin S$, $1 \in S$, and $x, y \in S$ implies that $xy \in S$. The **rings of fractions of** $R$ **with respect to** $S$, denoted $R[S^{-1}]$, is defined as follows.[11] Define an equivalence relation $\sim$ on $R \times S$ by $(r_1, s_1) \sim (r_2, s_2)$ when

$$r_1s_2 - r_2s_1 = 0.$$

[10] Alain M. Robert, *A Course in p-adic Analysis*, p. 18, §3.1.

[11] See M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Chapter 3.

It is immediate that $\sim$ is reflexive and symmetric. If $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$, then

$$r_1 s_2 - r_2 s_1 = 0, \qquad r_2 s_3 - r_3 s_2 = 0,$$

so, multiplying the first equation by $s_3$ and the second equation by $s_1$ we get $r_1 s_2 s_3 - r_2 s_1 s_3 = 0$ and $r_2 s_3 s_1 - r_3 s_2 s_1 = 0$ respectively. Combining these we get $r_1 s_2 s_3 = r_3 s_2 s_1$, i.e. $s_2(r_1 s_3 - r_3 s_1) = 0$. Because $s_2 \in S$, $s_2 \neq 0$, giving

$$r_1 s_3 - r_3 s_1 = 0,$$

showing that $\sim$ is transitive. We remark that $\sim$ being transitive does not use that $S$ is closed under multiplication.

For $(r, s) \in R \times S$, let $[(r, s)]$ be the equivalence class of $(r, s)$, and we define

$$R[S^{-1}] = (R \times S)/\sim = \{[(r, s)] : (r, s) \in R \times S\}.$$

We define

$$[(r_1, s_1)] + [(r_2, s_2)] = [(r_1 s_2 + r_2 s_1, s_1 s_2)].$$

Since $S$ is a multiplicative set, $s_1 s_2 \in S$. If $[(r_1, s_1)] = [(r_1', s_1')]$ and $[(r_2, s_2)] = [(r_2', s_2')]$, then $r_1 s_1' - r_1' s_1 = 0$ and $r_2 s_2' - r_2' s_2 = 0$ and thus

$$\begin{aligned}(r_1 s_2 + r_2 s_1)(s_1' s_2') - (r_1' s_2' + r_2' s_1')(s_1 s_2) &= r_1 s_2 s_1' s_2' + r_2 s_1 s_1' s_2' \\ &\quad - r_1' s_2' s_1 s_2 - r_2' s_1' s_1 s_2 \\ &= s_2 s_2'(r_1' s_1) + s_1 s_1'(r_2' s_2) \\ &\quad - r_1' s_2' s_1 s_2 - r_2' s_1' s_1 s_2 \\ &= 0,\end{aligned}$$

showing that this definition of addition of equivalence classes is well-defined. One then checks that addition in $R[S^{-1}]$ is associative, that $[(0, 1)]$ is the additive identity, that $-[(r, s)] = [(-r, s)]$, and that addition is commutative.

We define

$$[(r_1, s_1)] \cdot [(r_2, s_2)] = [(r_1 r_2, s_1 s_2)].$$

If $[(r_1, s_1)] = [(r_1', s_1')]$ and $[(r_2, s_2)] = [(r_2', s_2')]$, then $r_1 s_1' - r_1' s_1 = 0$ and $r_2 s_2' - r_2' s_2 = 0$ and thus

$$r_1 r_2 s_1' s_2' - r_1' r_2' s_1 s_2 = r_2 s_2'(r_1' s_1) - r_1' s_1 (r_2 s_2') = 0,$$

showing that this definition of multiplication of equivalence classes is well-defined. One then checks that multiplication in $R[S^{-1}]$ is associative, that $[(1, 1)]$ is the multiplicative identity, that multiplication is commutative, and that multiplication distributes over addition. This establishes that $R[S^{-1}]$ is a commutative ring with unity $[(1, 1)]]$.

Furthermore, if $[(r_1, s_1)] \cdot [(r_2, s_2)] = [(0, 1)]$, i.e. if $[(r_1 r_2, s_1 s_2)] = [(0, 1)]$, then $r_1 r_2 \cdot 1 - 0 \cdot s_1 s_2 = 0$, so $r_1 r_2 = 0$. Because $R$ is an integral domain, at

least one of $r_1, r_2$ is 0, and hence at least one of $[(r_1, s_1)], [(r_2, s_2)]$ is 0, showing that $R[S^{-1}]$ is an integral domain.

We define $j : R \to R[S^{-1}]$ by

$$j(x) = [(x, 1)], \qquad x \in R.$$

For $x, y \in R$,

$$j(x + y) = [(x + y, 1)] = [(x \cdot 1 + y \cdot 1, 1 \cdot 1)] = [(x, 1)] + [(y, 1)] = j(x) + j(y),$$

and

$$j(xy) = [(xy, 1)] = [(xy, 1 \cdot 1)] = [(x, 1)] \cdot [(y, 1)] = j(x)j(y),$$

and

$$j(1) = [(1, 1)],$$

showing that $j$ is a homomorphism of unital rings. If $j(x) = j(y)$ then $[(x, 1)] = [(y, 1)]$, giving $x \cdot 1 - y \cdot 1 = 0$, i.e. $x = y$, showing that $j$ is one-to-one. For $s \in S$,

$$j(s) \cdot [(1, s)] = [(s, 1)] \cdot [(1, s)] = [(s, s)] = [(1, 1)].$$

That is, $R$ is isomorphic as a ring to $j(R)$, $j(R)$ is a subring of $R[S^{-1}]$, and for any $s \in S$, $j(s)$ is invertible in $R[S^{-1}]$. Elements of $S$ need not be invertible in $R$, but elements of $j(S)$ are invertible in $R[S^{-1}]$.

Let $R$ be an integral domain, let $a \in R$ be nonzero, and let

$$S = \{a^k : k \in \mathbb{Z}_{\geq 0}\}.$$

$S$ is a multiplicative set, and we define

$$R[1/a] = R[S^{-1}],$$

called the **localization of $R$ away from $a$**. For example, for $a \in \mathbb{Z}$ nonzero, the map

$$[(m, s)] \mapsto \frac{m}{s}, \qquad m \in \mathbb{Z}, a \in S = \{a^k : k \in \mathbb{Z}_{\geq 0}\},$$

is a ring homomorphism $\mathbb{Z}[1/a] \to \mathbb{Q}$. We check that this map is one-to-one, and thus $\mathbb{Z}[1/a]$ is isomorphic as a ring to the collection of those $\frac{m}{s} \in \mathbb{Q}$ for which there is some $k \in \mathbb{Z}_{\geq 0}$ such that $s = a^k$.

# 8 The field of $p$-adic numbers

We now construct $\mathbb{Q}_p$. A **$p$-adic number** is a formal series of the form, for some $i_0 \in \mathbb{Z}$,

$$\sum_{i \geq i_0} a_i p^i, \qquad 0 \leq a_i \leq p_i - 1.$$

Thus, $\mathbb{Z}_p \subset \mathbb{Q}_p$, and, for example, $p^{-1}$ belongs to $\mathbb{Q}_p$ but does not belong to $\mathbb{Z}_p$. We extend the $p$-adic valuation $v_p : \mathbb{Z}_p \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ to $v_p : \mathbb{Q}_p \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by

defining $v_p(a)$ to be the least $i$ such that $a_i \neq 0$; indeed restricted to $\mathbb{Z}_p$ this is the $p$-adic valuation $\mathbb{Z}_p \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$. For nonzero $a \in \mathbb{Q}_p$ we have $p^{-v_p(a)}a = 0$, and hence we have that $p^{-v_p(a)}a \in \mathbb{Z}_p$. For $a, b \in \mathbb{Q}_p$, taking $\nu = \min\{v_p(a), v_p(b)\}$, we have $p^{-\nu}a + p^{-\nu}b \in \mathbb{Z}_p$, and we define $a + b = p^{\nu}(p^{-\nu}a + p^{-\nu}b) \in \mathbb{Q}_p$; that is, we have already established addition in $\mathbb{Z}_p$, and we define addition in $\mathbb{Q}_p$ using this addition in $\mathbb{Z}_p$. Likewise, for $\mu = v_p(a) + v_p(b)$, we have $(p^{-v_p(a)}a) \cdot (p^{-v_p(b)}b) \in \mathbb{Z}_p$, and we define $a \cdot b = p^{\mu}((p^{-v_p(a)}a) \cdot (p^{-v_p(b)}b)) \in \mathbb{Q}_p$. One then proves that with addition and multiplication thus defined, $\mathbb{Q}_p$ is a field.

For example, let us calculate the image of $\frac{5}{6} \in \mathbb{Q}$ in $\mathbb{Q}_3$. First, $\frac{5}{6} = 3^{-1} \cdot \frac{5}{2}$, and $\frac{5}{2} \in \mathbb{Z}_3$. We figure out that

$$2^{-1} = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4 + 1 \cdot 3^5 + \cdots \in \mathbb{Z}_3,$$

and then that

$$5 \cdot 2^{-1} = 1 + 2 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4 + 1 \cdot 3^5 + \cdots \in \mathbb{Z}_3.$$

Thus

$$\frac{5}{6} = 1 \cdot 3^{-1} + 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4 + \cdots \in \mathbb{Q}_3.$$

It was not luck that the digits $\frac{5}{6}$ in $\mathbb{Q}_3$ have a pattern: the digits of $x \in \mathbb{Q}_p$ are eventually periodic if and only if $x$ is the image in $\mathbb{Q}_p$ of some element of $\mathbb{Q}$.[12]

One proves that as unital rings,

$$\mathbb{Q}_p \cong \mathbb{Z}_p[1/p].$$

We define the **$p$-adic absolute value** $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_{\geq 0}$ by

$$|x|_p = p^{-v_p(x)}, \qquad x \in \mathbb{Q}_p.$$

Then we define the **$p$-adic metric** on $\mathbb{Q}_p$ by

$$d_p(x, y) = |x - y|_p, \qquad x, y \in \mathbb{Q}_p;$$

it is immediate that this is an extension of the $p$-adic metric on $\mathbb{Z}_p$. It can be proved that with the topology induced by the $p$-adic metric, $\mathbb{Q}_p$ is a topological field.[13] That is, $(x, y) \mapsto x + y$ is continuous $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$ is continuous, $x \mapsto -x$ is continuous $\mathbb{Q}_p \to \mathbb{Q}_p$, $(x, y) \mapsto x \cdot y$ is continuous $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$, and $x \mapsto x^{-1}$ is continuous $\mathbb{Q}_p^* \to \mathbb{Q}_p^*$. $\mathbb{Z}_p$ is a compact neighborhood of 0 in $\mathbb{Q}_p$, and because translation is a homeomorphism, it follows that each point in $\mathbb{Q}_p$ has a compact neighborhood, and thus that $\mathbb{Q}_p$ is locally compact. Furthermore,

$$\mathbb{Q}_p = \bigcup_{n \in \mathbb{Z}} p^n \mathbb{Z}_p,$$

showing that $\mathbb{Q}_p$ is $\sigma$-compact.

[12] See Alain M. Robert, *A Course in p-adic Analysis*, p. 39, §5.3.

[13] We have defined $\mathbb{Q}_p$ using $\mathbb{Z}_p$ and then defined a metric on $\mathbb{Q}_p$ and assigned $\mathbb{Q}_p$ the topology induced by this metric. $\mathbb{Q}_p$ is more satisfyingly constructed as a direct limit whose limitands are $\mathbb{Z}_p$, and this construction automatically gives $\mathbb{Q}_p$ a topology without us having to choose to use the $p$-adic metric. See Paul Garrett, *Classical definitions of $\mathbb{Z}_p$ and $\mathbb{A}$*, `http://www.math.umn.edu/~garrett/m/mfms/notes/05_compare_classical.pdf`

# 9 *p*-adic fractional parts

We identify the localization of $\mathbb{Z}$ away from $p$, $\mathbb{Z}[1/p]$, with the collection of rational numbers whose denominator is of the form $p^k, k \in \mathbb{Z}_{\geq 0}$. For example, $-\frac{6}{8} = -\frac{3}{4} \in \mathbb{Q}$ belongs to $\mathbb{Z}[1/2]$ but does not belong to $\mathbb{Z}[1/3]$. In particular, $\mathbb{Z} \subset \mathbb{Z}[1/p]$.

For $x \in \mathbb{Q}_p$, write

$$x = \sum_{i \geq v_p(x)} x_i p^i = \sum_{v_p(x) \leq i < 0} x_i p^i + \sum_{i \geq 0} x_i p^i = \{x\}_p + [x]_p.$$

$[x]_p$ is called the **integral part of** $x$ and $\{x\}_p$ is called the **fractional part of** $x$. We have $[x]_p \in \mathbb{Z}_p$. The fractional part $\{x\}_p$ satisfies

$$0 \leq \{x\}_p \leq \sum_{v_p(x) \leq i < 0} (p-1)p^i < 1,$$

and also $\{x\}_p \in \mathbb{Z}[1/p]$.

In the rest of this section we follow Conrad.[14] We use that fact that if $p, q$ are distinct primes, then $p \in \mathbb{Z}_q^*$ and hence

$$\mathbb{Z}[1/p] \subset \mathbb{Z}_q.$$

**Theorem 5.** *If $r \in \mathbb{Q}$, then*

$$r - \sum_p \{r\}_p \in \mathbb{Z}.$$

*Proof.* Let $q$ be prime. For prime $p \neq q$, we have $\{r\}_p \in \mathbb{Z}[1/p] \subset \mathbb{Z}_q$ and also $r - \{r\}_q = [r]_q \in \mathbb{Z}_q$. Therefore

$$r - \sum_p \{r\}_p = (r - \{r\}_q) - \sum_{p \neq q} \{r\}_p \in \mathbb{Z}_q.$$

Hence $q$ does not divide the denominator of $r - \sum_p \{r\}_p \in \mathbb{Q}$. But this is true for all prime $q$, which implies that $r - \sum_p \{r\}_p \in \mathbb{Z}$. □

We define $\psi_p : \mathbb{Q}_p \to S^1$ by

$$\psi_p(x) = e^{2\pi i \{x\}_p}, \qquad x \in \mathbb{Q}_p,$$

and we define $\psi_\infty : \mathbb{R} \to S^1$ by

$$\psi_\infty(x) = e^{-2\pi i x} = e^{-2\pi i \{x\}}, \qquad x \in \mathbb{R},$$

[14] Keith Conrad, *The character group of* $\mathbf{Q}$, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/characterQ.pdf`

where $[x]$ is the greatest integer $\leq x$ and $\{x\} = x - [x]$. It is immediate that $\psi_\infty$ is a homomorphism of topological groups. It satisfies $\psi_\infty(\mathbb{R}) = S^1$ and $\ker \psi_\infty = \mathbb{Z}$. The **first isomorphism theorem for topological groups** states that if $G$ and $H$ are topological groups and $f : G \to H$ is a homomorphism of topological groups that is onto and open, then $G/\ker f \cong H$ as topological groups.[15] The **open mapping theorem for topological groups** states that if $G$ and $H$ are locally compact topological groups, $f : G \to H$ is an onto homomorphism of topological groups, and $G$ is $\sigma$-compact, then $f$ is open.[16] These conditions are satisfied for $\psi_\infty : \mathbb{R} \to S^1$, so $\psi_\infty$ is open and therefore by the first isomorphism theorem,

$$\mathbb{R}/\mathbb{Z} \cong S^1$$

as topological groups.

**Theorem 6.** *If $p$ is prime then $\psi_p : \mathbb{Q}_p \to S^1$ is a homomorphism of topological groups.*

*Proof.* Let $x, y \in \mathbb{Q}_p$. We have

$$x - \{x\}_p = [x]_p, y - \{y\}_p = [y]_p, x + y - \{x + y\}_p = [x + y]_p \in \mathbb{Z}_p.$$

So

$$\begin{aligned}\{x\}_p + \{y\}_p - \{x + y\}_p &= (x - [x]_p) + (y - [y]_p) - (x + y - [x + y]_p) \\ &= [x + y]_p - [x]_p - [y]_p \in \mathbb{Z}_p.\end{aligned}$$

But $\{x\}_p + \{y\}_p - \{x + y\}_p \in \mathbb{Q}$, so the fact that it belongs to $\mathbb{Z}_p$ tells us that $p$ does not divide its denominator. On the other hand, because $\{x\}_p, \{y\}_p, \{x + y\}_p \in \mathbb{Z}[1/p]$, so $\{x\}_p + \{y\}_p - \{x + y\}_p \in \mathbb{Z}[1/p]$ and hence the denominator of $\{x\}_p + \{y\}_p - \{x + y\}_p \in \mathbb{Q}$ is of the form $p^k$, $k \in \mathbb{Z}_{\geq 0}$. Thus its denominator is 1, showing that $\{x\}_p + \{y\}_p - \{x + y\}_p \in \mathbb{Z}$, say $\{x + y\}_p = \{x\}_p + \{y\}_p + \nu$. Therefore

$$\psi_p(x+y) = e^{2\pi i\{x+y\}_p} = e^{2\pi i\{x\}_p + 2\pi i\{y\}_p + 2\pi i\nu} = e^{2\pi i\{x\}_p} e^{2\pi i\{y\}_p} = \psi_p(x)\psi_p(y),$$

showing that $\psi_p$ is a homomorphism of groups.

Because $\psi_p$ is a homomorphism of groups, to show that $\psi_p : \mathbb{Q}_p \to S^1$ is continuous it suffices to show that $\psi_p$ is continuous at $0 \in \mathbb{Q}_p$. For $|x|_p \leq 1 = p^0$, we have $v_p(x) \geq 0$, so $x \in \mathbb{Z}_p$ and hence $\{x\}_p = 0$. Thus, for $|x|_p \leq 1$ we have $\psi_p(x) = 1 = \psi_p(0)$, showing that $\psi_p$ is continuous at 0 and therefore that $\psi_p : \mathbb{Q}_p \to S^1$ is continuous. (Namely, because $\psi_p$ is a homomorphism of groups, what we have established shows that it is **locally constant**.) □

[15] Dikran Dikranjan, *Introduction to Topological Groups*, `http://users.dimi.uniud.it/~dikran.dikranjan/ITG.pdf`, p. 21, Theorem 3.4.2; Karl Heinrich Hofmann, *Introduction to Topological Groups*, `http://www.mathematik.tu-darmstadt.de/lehrmaterial/SS2006/CompGroups/topgr.pdf`, p. 35, Chapter 3.

[16] Dikran Dikranjan, *Introduction to Topological Groups*, `http://users.dimi.uniud.it/~dikran.dikranjan/ITG.pdf`, p. 42, Theorem 7.2.8.

For $x \in \mathbb{Q}_p$ we have $\{x\}_p \in \mathbb{Z}[1/p]$, say $\{x\}_p = \frac{a}{p^k}$, for some $a \in \mathbb{Z}$ and $k \in \mathbb{Z}_{\geq 0}$, which implies that

$$(\psi_p(x))^{p^k} = (e^{2\pi i a/p^k})^{p^k} = e^{2\pi i a} = 1 \in S^1.$$

Therefore,

$$\psi_p(x) \in \mathbb{Z}(p^\infty),$$

the Prüfer $p$-group. One checks that

$$\psi_p(\mathbb{Q}_p) = \mathbb{Z}(p^\infty)$$

and that

$$\ker \psi_p = \mathbb{Z}_p.$$

$\mathbb{Z}(p^\infty)$ is a discrete abelian group and thus is locally compact. $\mathbb{Q}_p$ is locally compact (because $x + \mathbb{Z}_p$ is a compact neighborhood of $x \in \mathbb{Q}_p$) and $\sigma$-compact (because $\mathbb{Q}_p$ is equal to a countable union of dilations of $\mathbb{Z}_p$). Thus the conditions of the open mapping theorem are satisfied for $\psi_p : \mathbb{Q}_p \to \mathbb{Z}(p^\infty)$, so $\psi_p$ is open. Therefore by the first isomorphism theorem,

$$\mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Z}(p^\infty)$$

as topological groups.

In Theorem 6 we proved that the map $x \mapsto e^{2\pi i\{x\}_p}$ belongs to $\widehat{\mathbb{Q}_p}$, the Pontryagin dual of the additive locally compact abelian group $\mathbb{Q}_p$. For $y \in \mathbb{Q}_p$, define

$$\xi_{p,y} : \mathbb{Q}_p \to S^1$$

by

$$\xi_{p,y}(x) = \psi_p(xy) = e^{2\pi i\{xy\}_p}, \qquad x \in \mathbb{Q}_p,$$

and we check that $\xi_{p,y} \in \widehat{\mathbb{Q}_p}$. It can in fact be proved that $y \mapsto \xi_{p,y}$ is an isomorphism of topological groups $\mathbb{Q}_p \to \widehat{\mathbb{Q}_p}$.[17]

# 10 The ring of adeles

We define $\mathbb{A}$ to be the set of those $x \in \mathbb{R} \times \prod_p \mathbb{Q}_p$ such that $\{p : x_p \notin \mathbb{Z}_p\}$ is finite. This is an instance of a **restricted direct product**. For example, $x$ defined by $x_\infty = \sqrt{3}$, $x_2 = \frac{1}{2}$, and $x_p = 1$ for $p > 2$ belongs to $\mathbb{A}$, while $x_\infty = \sqrt{3}$, $x_p = \frac{1}{p}$ does not belong to $\mathbb{A}$. Elements of $\mathbb{A}$ are called **adeles**. It is apparent that with addition and multiplication defined pointwise, $\mathbb{A}$ is a commutative ring, with additive identity $x_\infty = 0, x_p = 0$ for all $p$ and unity $x_\infty = 1$, $x_p = 1$ for all $p$. We assign $\mathbb{A}$ the topology generated by the base of subsets of $\mathbb{A}$ of the form

$$\Omega_\infty \times \prod_{p \in S} \Omega_p \times \prod_{p \notin S} \mathbb{Z}_p,$$

[17] Gerald B. Folland, *A Course in Abstract Harmonic Analysis*, p. 92, Theorem 4.12.

where $S$ is a finite set of primes, $\Omega_p$ is an open subset of $\mathbb{Q}_p$, and $\Omega_\infty$ is an open subset of $\mathbb{R}$.[18] With this topology, $\mathbb{A}$ is a locally compact topological ring.[19] In particular, the additive group $\mathbb{A}$ is a locally compact abelian group.

The map $s \mapsto x \in \mathbb{A}$ with $x_\infty = s$, $x_p = s$ for all $p$, is a homomorphism of topological unital rings $\mathbb{Q} \to \mathbb{A}$. (It is immediate that it is a homomorphism of unital rings, and it is continuous because $\mathbb{Q}$ is discrete.) We identify $\mathbb{Q}$ with those elements $x$ of $\mathbb{A}$ for which there is some $s \in \mathbb{Q}$ such that $x_\infty = s$ and $x_p = s$ for all prime $p$, which are called **rational adeles**.

For $x \in \mathbb{A}$, we define $\Psi_x : \mathbb{Q} \to S^1$ by

$$\Psi_x(r) = \psi_\infty(rx_\infty) \cdot \prod_p \psi_p(rx_p), \qquad r \in \mathbb{Q}.$$

This is a homomorphism of topological groups, because each factor is a homomorphism of topological groups and for any $x \in \mathbb{A}$ and $r \in \mathbb{Q}$, the number of factors that are not equal to 1 is finite.

**Lemma 7.** *$x \mapsto \Psi_x$ is a homomorphism of topological groups $\mathbb{A} \to \widehat{\mathbb{Q}}$.*

*Proof.* Let $x, y \in \mathbb{A}$. For $r \in \mathbb{Q}$, because $\psi_\infty$ and the $\psi_p$ are homomorphisms,

$$\begin{aligned}\Psi_{x+y}(r) &= \psi_\infty(rx_\infty + ry_\infty) \cdot \prod_p \psi_p(rx_p + ry_p) \\ &= \psi_\infty(rx_\infty)\psi_\infty(ry_\infty) \prod_p (\psi_p(rx_p)\psi_p(ry_p)) \\ &= \Psi_x(r)\Psi_y(r),\end{aligned}$$

showing that $x \mapsto \Psi_x$ is a homomorphism of groups.

To show that $x \mapsto \Psi_x$ is continuous $\mathbb{A} \to \widehat{\mathbb{Q}}$, it suffices to show that it is continuous at $0 \in \mathbb{A}$. Generally, if $G$ is a locally compact abelian group, it is a fact that a local base at 0 for the topology of $\widehat{G}$ is the collection of sets of the form

$$N(K, \epsilon) = \{\gamma \in \widehat{G} : \text{if } g \in K \text{ then } |1 - \gamma(g)| < \epsilon\},$$

where $K$ is a compact subset of $G$ and $\epsilon > 0$.[20] Let $K$ be a compact subset of $\mathbb{Q}$ and let $\epsilon > 0$. $\mathbb{Q}$ is discrete so $K$ is finite; take $R = \max\{|r| : r \in K\}$ and let $S$ be the set of those primes $p$ for which there is some $r \in K$ with $r \notin \mathbb{Z}_p$. Because $\psi_\infty : \mathbb{R} \to S^1$ is continuous and $K$ is finite, there is an open neighborhood $\Omega_\infty$ of $0 \in \mathbb{R}$ such that if $x_\infty \in \Omega_\infty$ and $r \in K$ then $|1 - \psi_\infty(rx_\infty)| < \epsilon$. Furthermore, because $K$ is finite, the set $S$ is finite and

[18] It is not apparent why we ought to use this topology. $\mathbb{A}$ can instead be defined as a direct limit of topological rings $\mathbb{A}_S$, where $S$ is a finite subset of $\{\infty\} \cup \{\text{prime numbers}\}$. See Paul Garrett, *Classical definitions of $\mathbb{Z}_p$ and $\mathbb{A}$*, `http://www.math.umn.edu/~garrett/m/mfms/notes/05_compare_classical.pdf`

[19] cf. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, p. 519, Appendix I, Lemma 1; Anton Deitmar, *Automorphic Forms*, Chapter 5; Anthony W. Knapp, *Advanced Real Analysis*, Chapter VI.

[20] Walter Rudin, *Fourier Analysis on Groups*, p. 10, §1.2.6.

therefore for each $p \in S$ there is some $\nu_p \in \mathbb{Z}_{\geq 0}$ such that if $r \in K$ then $p^{\nu_p} r \in \mathbb{Z}_p$. Let $\Omega_p = p^{\nu_p}\mathbb{Z}_p$. Then, for $x_p \in \Omega_p$ and $r \in K$ we have $rx_p \in \mathbb{Z}_p$. It follows that if $x \in \Omega_\infty \times \prod_{p\in S} \Omega_p \times \prod_{p\notin S} \mathbb{Z}_p$ then for all $r \in K$ we have then $|1 - \Psi_x(r)| < \epsilon$. That is, $x \in \Omega_\infty \times \prod_{p\in S} \Omega_p \times \prod_{p\notin S} \mathbb{Z}_p$ implies that $\Psi_x \in N(K, \epsilon)$, showing that $x \mapsto \Psi_x$ is continuous at 0, and therefore that $x \mapsto \Psi_x : \mathbb{A} \to \widehat{\mathbb{Q}}$ is continuous. □

**Theorem 8.** *For every $\chi \in \widehat{\mathbb{Q}}$ there is some $x \in \mathbb{A}$ such that $\chi = \Psi_x$, and* $\ker \Psi = \mathbb{Q}$.

*Proof.* There is a unique $x_\infty \in [0, 1)$ such that $\chi(1) = e^{-2\pi i x_\infty} = \psi_\infty(x_\infty)$. Define $\chi_\infty : \mathbb{Q} \to S^1$ by

$$\chi_\infty(r) = \psi_\infty(rx_\infty) = e^{-2\pi i r x_\infty}, \qquad r \in \mathbb{Q}.$$

Then $\chi_\infty \in \widehat{\mathbb{Q}}$ and $\chi_\infty(1) = \chi(1)$. Further, define $\gamma : \mathbb{Q} \to S^1$ by

$$\gamma(r) = \frac{\chi(r)}{\chi_\infty(r)}, \qquad r \in \mathbb{Q}.$$

Then $\gamma \in \widehat{\mathbb{Q}}$, $\gamma(1) = 1$, and $\chi(r) = \chi_\infty(r)\gamma(r)$. By Theorem 5, for any $s \in \mathbb{Q}$ we have

$$e^{2\pi i s} = \prod_p e^{2\pi i \{s\}_p}.$$

For $r \in \mathbb{Q}$, let $s_r \in \mathbb{Q}$ such that $\gamma(r) = e^{2\pi i s_r}$. We define $\chi_p : \mathbb{Q} \to S^1$ by

$$\chi_p(r) = \psi_p(s_r) = e^{2\pi i \{s_r\}_p}, \qquad r \in \mathbb{Q}.$$

One checks that $\chi_p \in \widehat{\mathbb{Q}}$. For any $r \in \mathbb{Q}$,

$$\gamma(r) = e^{2\pi i s_r} = \prod_p e^{2\pi i \{s_r\}_p} = \prod_p \chi_p(r),$$

whence

$$\chi(r) = \chi_\infty(r) \cdot \prod_p \chi_p(r).$$

Let $p$ be prime. For $n \geq 1$, using $\chi_p(1) = e^{2\pi i \{1\}_p} = 1$ we have $\chi_p(p^{-n})^{p^n} = \chi_p(1) = 1$, and hence there is a unique $c_n$, $0 \leq c_n \leq p^n - 1$, such that

$$\chi_p\left(\frac{1}{p^n}\right) = e^{\frac{2\pi i c_n}{p^n}}.$$

For $n \geq m$,

$$\chi_p\left(\frac{1}{p^n}\right)^{p^{n-m}} = \chi_p\left(\frac{1}{p^m}\right) = e^{\frac{2\pi i c_m}{p^m}},$$

which yields $\frac{c_n}{p^m} - \frac{c_m}{p^m} \in \mathbb{Z}$, i.e. $c_n - c_m \in p^m\mathbb{Z}$, i.e. $|c_n - c_m|_p \leq p^{-m}$. It follows that $c_n$ is a Cauchy sequence in $(\mathbb{Z}, d_p)$, and therefore there is some $x_p \in \mathbb{Z}_p$

such that $c_n \to x_p$ in $\mathbb{Z}_p$. This limit $x_p$ satisfies $x_p - c_n \in p^n\mathbb{Z}_p$ for all $n$, so $\frac{x_p}{p^n} - \frac{c_n}{p^n} \in \mathbb{Z}_p$ for all $n$, hence, as $0 \le c_n \le p^n - 1$,

$$\left\{\frac{x_p}{p^n}\right\}_p = \left\{\frac{c_n}{p^n}\right\}_p = \frac{c_n}{p^n}, \qquad n \ge 1. \tag{2}$$

Let $r = \frac{a}{b} \in \mathbb{Q}$, $\gcd(a,b) = 1$ and let $b = p^n\beta$ with $n = v_p(b)$. Then, because $\chi_p \in \widehat{\mathbb{Q}}$ and by the definition of $c_n$,

$$\chi_p(r)^\beta = \chi_p(\beta r) = \chi_p\left(\frac{a}{p^n}\right) = \chi_p\left(\frac{1}{p^n}\right)^a = \left(e^{\frac{2\pi i c_n}{p^n}}\right)^a = \exp\left(\frac{2\pi i a c_n}{p^n}\right).$$

Furthermore, by (2) we have

$$\frac{ac_n}{p^n} + \mathbb{Z} = a \cdot \left\{\frac{x_p}{p^n}\right\}_p + \mathbb{Z} = \left\{\frac{ax_p}{p^n}\right\}_p + \mathbb{Z} = \{\beta r x_p\}_p + \mathbb{Z} = \beta\{rx_p\}_p + \mathbb{Z},$$

so

$$\chi_p(r)^\beta = \exp\left(\frac{2\pi i a c_n}{p^n}\right) = \exp(2\pi i\beta\{rx_p\}_p) = \exp(2\pi i\{rx_p\}_p)^\beta,$$

giving

$$\left(\frac{\chi_p(r)}{\exp(2\pi i\{rx_p\}_p)}\right)^\beta = 1.$$

But $\chi_p(r)$ and $\exp(2\pi i\{rx_p\}_p)$ are both $p$th roots of unity and $\gcd(\beta, p) = 1$, so this implies that

$$\chi_p(r) = \exp(2\pi i\{rx_p\}_p) = \psi_p(rx_p), \qquad r \in \mathbb{Q}.$$

Then $x$ thus defined belongs to $\mathbb{A}$, and for any $r \in \mathbb{Q}$,

$$\Psi_x(r) = \psi_\infty(rx_\infty) \cdot \prod_p \psi_p(rx_p) = \chi_\infty(r) \cdot \prod_p \chi_p(r) = \chi(r).$$

Therefore $\Psi_x = \chi$.

On the other hand, suppose that $x, y \in [0,1) \times \prod_p \mathbb{Z}_p$ and that $\Psi_x = \Psi_y$. Because $x_p \in \mathbb{Z}_p$ for each prime $p$,

$$\Psi_x(1) = \psi_\infty(x_\infty) \cdot \prod_p \psi_p(x_p) = e^{-2\pi i x_\infty} \cdot \prod_p e^{2\pi i\{x_p\}_p} = e^{-2\pi i x_\infty},$$

and likewise $\Psi_y(1) = e^{-2\pi i y_\infty}$. As $e^{-2\pi i x_\infty} = e^{-2\pi i y_\infty}$ and $x_\infty, y_\infty \in [0,1)$, it follows that $x_\infty = y_\infty$. Let $p$ be prime and let $n \ge 0$. On the one hand, for

$q \neq p$ we have $p^{-n}x_q \in \mathbb{Z}_q$, whence, as $x_\infty = y_\infty$,

$$\begin{aligned}\frac{\Psi_x(p^{-n})}{\Psi_y(p^{-n})} &= \frac{\psi_\infty(p^{-n}x_\infty)\cdot\prod_q \psi_q(p^{-n}x_p)}{\psi_\infty(p^{-n}y_\infty)\cdot\prod_q \psi_q(p^{-n}y_p)} \\ &= \frac{\psi_\infty(p^{-n}x_\infty)\cdot\psi_p(p^{-n}x_p)}{\psi_\infty(p^{-n}y_\infty)\cdot\psi_p(p^{-n}y_p)} \\ &= \frac{\psi_p(p^{-n}x_p)}{\psi_p(p^{-n}y_p)} \\ &= e^{2\pi i\{p^{-n}x_p\}_p - 2\pi i\{p^{-n}y_p\}_p}.\end{aligned}$$

But $\Psi_x = \Psi_y$, so $\{p^{-n}x_p\}_p - \{p^{-n}y_p\}_p \in \mathbb{Z}$, and since $0 \leq \{\cdot\}_p < 1$ this means

$$\{p^{-n}x_p\}_p = \{p^{-n}y_p\}_p.$$

Because this is true for each $n \geq 0$, it follows that $x_p = y_p$. Therefore, $x = y$.

Let $x \in \mathbb{A}$ and suppose that if $p \notin S$ then $x_p \in \mathbb{Z}_p$. Define

$$s = \sum_{p\in S}\{x_p\}_p.$$

Then for all prime $p$ we have $\{x_p - s\}_p = 0$ and so $x_p - s \in \mathbb{Z}_p$. Therefore $x - s \in \mathbb{R}\times\prod_p \mathbb{Z}_p$. Let $N = [x_\infty - s]$, with which $x_\infty - (s+N) = (x_\infty - s) - N \in [0,1)$. For any prime $p$ we have $N \in \mathbb{Z}_p$ and so, as $x_p - s \in \mathbb{Z}$, we have $x_p - (s+N) = (x_p - s) - N \in \mathbb{Z}_p$. Thus

$$x - (s+N) \in [0,1)\times\prod_p \mathbb{Z}_p,$$

and therefore

$$\mathbb{A} = \mathbb{Q} + [0,1)\times\prod_p \mathbb{Z}_p.$$

For $s \in \mathbb{Q} \subset \mathbb{A}$ and $r \in \mathbb{Q}$, then by Theorem 5,

$$\begin{aligned}\Psi_s(r) &= \psi_\infty(rs)\cdot\prod_p \psi_p(rs) \\ &= e^{-2\pi irs}\cdot\prod_p e^{2\pi i\{rs\}_p} \\ &= 1.\end{aligned}$$

Hence $\mathbb{Q} \subset \ker\Psi$. □

$\mathbb{A}$ is a $\sigma$-compact locally compact abelian group and $\Psi : \mathbb{A} \to \widehat{\mathbb{Q}}$ is an onto homomorphism of topological groups, so by the open mapping theorem for topological groups, $\Psi$ is open. Then by the first isomorphism theorem for topological groups, because $\ker\Psi = \mathbb{Q}$, we have

$$\widehat{\mathbb{Q}} \cong \mathbb{A}/\mathbb{Q}$$

as topological groups.