Construction of $\mathbb{Q}_p$ with Two Approaches

Lanqi Fei

University of Maryland

lanqifei@terpmail.umd.edu

Why do we study P-adic Numbers?

- The p-adic numbers is a larger number system containing $\mathbb{Q}$, with nicer properties.

Why do we study P-adic Numbers?

- The p-adic numbers is a larger number system containing $\mathbb{Q}$, with nicer properties.

- When the p-adic numbers were introduced they considered as an exotic part of pure mathematics without any application.

Why do we study P-adic Numbers?

- The p-adic numbers is a larger number system containing $\mathbb{Q}$, with nicer properties.
- When the p-adic numbers were introduced they considered as an exotic part of pure mathematics without any application.
- It turns out later to have powerful applications in fields like number theory, including, for example, in the famous proof of **Fermat's Last Theorem** by Andrew Wiles.

Why do we study P-adic Numbers?

- The p-adic numbers is a larger number system containing $\mathbb{Q}$, with nicer properties.
- When the p-adic numbers were introduced they considered as an exotic part of pure mathematics without any application.
- It turns out later to have powerful applications in fields like number theory, including, for example, in the famous proof of **Fermat's Last Theorem** by Andrew Wiles.
- Since 80th p-adic numbers are used in applications to **quantum physics**.

Overview

1. Algebraic Construction
2. Topological Construction
3. Connecting the Two Constructions

Algebraic Construction

P-adic Integer

Given a prime p, for each integer m, we can write it in base p in a unique way,

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n, \quad 0 \leq a_i < p$$

- **Example**

$$7 = 1 + 1 \cdot 2 + 1 \cdot 2^2$$

P-adic Integer

Definition (P-adic Integer)

Let p be a prime. The set of **p-adic integers** is defined as

$$\mathbb{Z}_p = \left\{ a_0 + a_1 p + a_2 p^2 + \dots \right\}$$

where $0 \leq a_i < p$

- **Example**

$$1 + 1 \cdot 2 + 1 \cdot 2^2 + \cdots + 1 \cdot 2^n + \cdots \in \mathbb{Z}_2$$

P-adic Integer

$$a_0 + a_1 p + a_2 p^2 + \dots$$
$$\downarrow \quad \text{mod } p^n$$
$$[a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}] \in \mathbb{Z}/p^n\mathbb{Z}$$

where $0 \leq a_i < p$

P-adic Integer

This defines a map from $\mathbb{Z}_p$ to $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$

$$\sum_{i=0}^{\infty} a_i p^i \longmapsto ([a_0], [a_0 + a_1 p], \ldots, [\sum_{i=0}^{n-1} a_1 p^i], [\sum_{i=0}^{n} a_1 p^i], \ldots)$$

P-adic Integer

This defines a map from $\mathbb{Z}_p$ to $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$

$$\sum_{i=0}^{\infty} a_i p^i \longmapsto ([a_0], [a_0 + a_1 p], \ldots, [\sum_{i=0}^{n-1} a_1 p^i], [\sum_{i=0}^{n} a_1 p^i], \ldots)$$

Moreover, we have

$$[\sum_{i=0}^{n} a_1 p^i] \quad \xmapsto{\bmod p^{n-1}} \quad [\sum_{i=0}^{n-1} a_1 p^i]$$

Inverse Limit

Definition

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid x_n \mapsto x_{n-1}, n = 1, 2, \ldots \right\}$$

Inverse Limit

Theorem

Associating to every p-adic integer $a = \sum_{i=0}^{\infty} a_i p^i$ *the sequence* $(x_n)_{n\in\mathbb{N}}$ *of equivalence classes*

$$x_n = \sum_{i=0}^{n-1} a_i p^i \mod p^n \in \mathbb{Z}/p^n\mathbb{Z},$$

yields a bijection

$$\mathbb{Z}_p \longrightarrow \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

- **Example**

$$1 + 2 + 2^2 + \cdots + 2^n + \ldots \longleftrightarrow ([1], [1+2], [1+2+2^2], \ldots)$$
$$= (1 \mod 2, 3 \mod 4, \ldots)$$

P-adic Numbers

Definition

we extend the domain of p-adic integers into that of the formal series

$$\sum_{v=-m}^{\infty} a_v p^v = a_{-m}p^{-m} + \cdots + a_0 + a_1 p + \ldots,$$

where $m \in \mathbb{Z}$ and $0 \leq a_v < p$. We call such series **p-adic numbers** and denote the set of p-adic numbers as $\mathbb{Q}_p$.

Topological Construction

Motivation

$\mathbb{R} \equiv$ completion of $\mathbb{Q}$ with respect to the usual absolute value $|\ |$, which has the following properties

1. $|a| = 0 \Leftrightarrow a = 0$
2. $|ab| = |a||b|$
3. $|a + b| \leq |a| + |b|$

We'll construct p-adic numbers in a similar way, with a different absolute value.

P-adic Absolute Value

Definition (P-adic Absolute Value)

Let p be a prime. Given a non-zero rational $x = \frac{m}{n}$, where $m, n \in \mathbb{Z}$,we can write it as follows,

$$x = p^{v_p(x)} \frac{a'}{b'}$$

such that $p \not| a'$ and $p \not| b'$.

The **p-adic absolute value** is defined as follows,

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

and we define $|0|_p = 0$.

P-adic Absolute Value

- **Example**

$$125 = 5^3 \qquad\qquad 3 = 5^0 \times 3$$

$$|125|_5 = 5^{-3} \qquad\qquad |3|_5 = 5^0 = 1$$

$$\Downarrow$$

$$|125|_5 < |3|_5!$$

Absolute Values on $\mathbb{Q}$

Theorem (Ostrowski's)

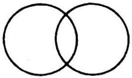
Every non-trivial absolute value on $\mathbb{Q}$ is either $|\ |_p$ for some prime p or the usual absolute value $|\ |$.

Topology

In $(\mathbb{Q}, d)$, $d(x, y) = |x - y|_p$

- All triangles are isosceles.
- Any point of ball $B(a, r) = \{x \in \mathbb{Q} : |x - a|_p \leq r\}$ is center.
- Two balls are either disjoint, or one is contained in the other.

These are allowed...



but not this!

Completion

Definition

$$\mathcal{C} = \left\{ \text{Cauchy Sequences in } \mathbb{Q} \text{ w.r.t } |\ |_p \right\} = \{(c_1, c_2, \dots)\}$$

$$\begin{aligned} \mathfrak{m} &= \left\{ \text{Nullsequences in } \mathbb{Q} \right\} \\ &= \{(x_1, x_2, \dots) \mid |x_n|_p \to 0\} \end{aligned}$$

Completion

Definition

$$
\begin{aligned}
\mathcal{C} &= \left\{\text{Cauchy Sequences in } \mathbb{Q} \text{ w.r.t } |\ |_p\right\} = \{(c_1, c_2, \dots)\} \\
\mathfrak{m} &= \left\{\text{Nullsequences in } \mathbb{Q}\right\} \\
&= \{(x_1, x_2, \dots) \mid |x_n|_p \to 0\}
\end{aligned}
$$

Theorem

$\mathcal{C}$ forms a ring, and $\mathfrak{m}$ forms a maximal ideal of $\mathcal{C}$.

Completion

Definition

We define the field of **p-adic numbers** to be

$$\mathbb{Q}_p \equiv \mathcal{C}/\mathfrak{m}$$

Completion

Definition

We define the field of **p-adic numbers** to be

$$\mathbb{Q}_p \equiv \mathcal{C}/\mathfrak{m}$$

We extend the p-adic absolute value to $\mathbb{Q}_p$ by setting

$$|x|_p = |(x_1, x_2, \dots) + \mathfrak{m}|_p = \lim_{n\to\infty} |x_n|_p$$

Completion

Theorem

The field $\mathbb{Q}_p$ of p-adic numbers is **complete** *with respect to the absolute value $|\ |_p$, i.e., every Cauchy sequence in $\mathbb{Q}_p$ converges with respect to $|\ |_p$.*

P-adic Integers

Definition

The set of **p-adic integers** is defined as

$$\mathbb{Z}_p := \left\{ x \in \mathbb{Q}_p \;\middle|\; |x|_p \leq 1 \right\}$$

is a subring of $\mathbb{Q}_p$. It is the closure with respect to $|\ |_p$ of the ring $\mathbb{Z} \subset \mathbb{Q}_p$.

P-adic Integers

Theorem

The non-zero ideals of the ring $\mathbb{Z}_p$ *are the principal ideals*

$$p^n\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p \mid |x|_p \leq \frac{1}{p^n}\right\}$$

with $n \geq 0$*, and we have*

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

Isomorphism

Theorem (Cont.)

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

$$[x] \leftrightarrow [a]$$

where $a \in \mathbb{Z}$ satisfies $|x-a|_p \leq \frac{1}{p^n}$, and $[a] \in \mathbb{Z}/p^n\mathbb{Z}$ is unique.

Connecting the Two Constructions

Connecting Two Approaches

For each n, we get a homomorphism

$$\begin{array}{ccccc} \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p/p^n\mathbb{Z}_p & \cong & \mathbb{Z}/p^n\mathbb{Z} \\ x & \longmapsto & [x] & \longleftrightarrow & [a_n] \end{array}$$

Connecting Two Approaches

For each n, we get a homomorphism

$$\begin{array}{ccccc} \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p/p^n\mathbb{Z}_p & \cong & \mathbb{Z}/p^n\mathbb{Z} \\ x & \longmapsto & [x] & \longleftrightarrow & [a_n] \end{array}$$

Combine the homomorphisms for all n, we get a homomorphism

$$\mathbb{Z}_p \longrightarrow \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$$

In fact, the we get

$$\mathbb{Z}_p \longrightarrow \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

Connecting Two Approaches

Theorem

The homomorphism

$$\mathbb{Z}_p \longrightarrow \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

is an isomorphism (and even homeomorphism).

- LHS = Topological definition of p-adic integers
- RHS = Algebraic definition of p-adic integers

Connecting Two Approaches

For the algebraic side, we define $\mathbb{Q}_p$ to be the quotient field of p-adic integers; for the topological side, we can prove $\mathbb{Q}_p =$ quotient field of $\mathbb{Z}_p$.

Because the two rings are isomorphic, their quotient fields are isomorphic, so two definitions of p-adic numbers coincide.

References

Fernando Q. Gouvea (1997)
p-adic Numbers: An Introduction

Jurgen Neukirch (1999)
Algebraic Number Theory

U. A. Rozikov (2013)
What are p-adic Numbers? What are They Used for?

Thank You