The Complex p-Adic Numbers

Luke Saharia, Durham University

February 7th, 2024

Table of Contents

Table of Contents

Important Note

For the entirety of this presentation, p will be a prime number.

Introduction

$$
\begin{tikzcd}
 & \mathbb{Q} \arrow[dl, dash, "p\text{-adic Completion}"'] \arrow[dr, dash, "\text{Euclidean Completion}"] & \\
\mathbb{Q}_p \arrow[d, dash, "\text{Algebraic Closure}"'] & & \mathbb{R} \arrow[d, dash, "\text{Algebraic Closure}"] \\
\overline{\mathbb{Q}}_p \arrow[d, dash, "p\text{-adic Completion}"'] & & \mathbb{C} \\
\mathbb{C}_p & &
\end{tikzcd}
$$

Table of Contents

Field Norms

Definition (Norm on a field)

For F a field, a function $\|\cdot\| : F \to \mathbb{R}_{\geq 0}$ is called a field norm if the following are satisfied for all $x, y \in F$:

- $\|x\| = 0 \iff x = 0$ (Positive-definiteness)
- $\|xy\| = \|x\| \cdot \|y\|$ (Multiplicativity)
- $\|x + y\| \leq \|x\| + \|y\|$ (Triangle Inequality)

We call a field with a norm a *normed field*.

Example

The absolute value with the rational numbers, $(\mathbb{Q}, |\cdot|)$, is a normed field.

Cauchy Sequences and Completeness

Theorem

The completion of a normed field is itself a normed field, with continuous extensions of the field operations, $+$, $\times$ and the norm, $\|\cdot\|$.

p-Adic Norm

For any $x \in \mathbb{Q}^x$ we can uniquely write it as

$$x = p^n \frac{a}{b}, \qquad \text{where } a, b \in \mathbb{Z} \text{ and } p \nmid a \text{ or } b$$

Definition (p-Adic Norm)

For any $x \in \mathbb{Q}^x$, $x = p^n \frac{a}{b}$, we define the p-adic norm of x to be $|x|_p := \frac{1}{p^n}$.
For $x = 0$, we define $|0|_p = 0$.

The p-adic norm satisfies the following:

- $|x|_p = 0 \iff x = 0$ (Positive-definiteness)
- $|xy|_p = |x|_p \cdot |y|_p$ (Multiplicativity)
- $|x + y|_p \leq \max(|x|_p, |y|_p) \leq |x|_p + |y|_p$ (Strong Triangle Inequality)

Examples

$|27|_3 = \frac{1}{27}$, $\quad |9|_7 = 1$, $\quad \left|\frac{17x3}{8}\right|_2 = 8$, $\quad \left|\frac{17x3}{8}\right|_{17} = \frac{1}{17}$, $\quad |p!|_p = \frac{1}{p}$

Table of Contents

$\mathbb{Q}$ is Not 7-Adically Complete

We can construct a sequence of rational numbers $(x_n)_{n\in\mathbb{N}}$ satisfying:

1. $x_n^2 + 3 \equiv 0 \mod 7^n$
2. $x_{n+1} \equiv x_n \mod 7^n$

The sequence is Cauchy with respect to $|\cdot|_7$.
Let

$$\ell := \lim_{n\to\infty} x_n,$$

then $\ell^2 = -3$, so $\ell \notin \mathbb{Q}$.

The p-Adic Completion of $\mathbb{Q}$

Definition

The p-adic completion of $\mathbb{Q}$ is the p-adic numbers, denoted $\mathbb{Q}_p$.

Lemma (p-adic expansion)

There is a **unique** p-adic expansion of $x \in \mathbb{Q}_p$:

$$x = \sum_{k=m}^{\infty} a_k p^k,$$

for some $m \in \mathbb{Z}$ and the $a_k's$ taken from a certain set of "digits".

Teichmüller Representatives

Definition (Teichmüller Representatives)

The Teichmüller representatives in $\mathbb{Q}_p$ are 0 and the $(p-1)$th roots of unity in $\mathbb{Z}_p$. They all satisfy

$$x^p - x = 0.$$

Remark

The Teichmüller representatives form a complete set of residues modulo p.

Table of Contents

The Ring of Integers and Residue Field

Lemma

Finite extensions K of $\mathbb{Q}_p$ are complete fields and $|\cdot|_p$ uniquely extends to K.

Definition

Let K be a finite extension of $\mathbb{Q}_p$. Then

- $\mathcal{O}_K = \left\{x \in K \mid |x|_p \leq 1\right\}$ is the **ring of integers** in K.
- $\mathfrak{m} = \left\{x \in K \mid |x|_p < 1\right\}$ is the **unique maximal ideal** in $\mathcal{O}_K$.
- $k = \mathcal{O}_K/\mathfrak{m}$ is the **residue field** of K.

Examples

Taking $K = \mathbb{Q}_p$ then: $\mathcal{O}_K = \mathbb{Z}_p$, $\mathfrak{m} = p\mathbb{Z}_p$, $k = \mathcal{O}_K/\mathfrak{m} = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.

Unramified Extensions of $\mathbb{Q}_p$

Definition (Unramified Extension)

Let $K/\mathbb{Q}_p$ be a finite extension, then $k/\mathbb{F}_p$ is an extension of finite fields. We call K an **unramified** extension of $\mathbb{Q}_p$ if $[K : \mathbb{Q}_p] = [k : \mathbb{F}_p]$.

Theorem (Classification of Unramified Extensions)

Let $K/\mathbb{Q}_p$ be an unramified extension. Then $K = \mathbb{Q}_p(\zeta_n)$ for some n coprime to p and ζ_n a primitive nth root of unity.

Definition (Teichmüller Representatives in $K/\mathbb{Q}_p$)

For K a finite extension of $\mathbb{Q}_p$. The elements from $k = \mathcal{O}_K/\mathfrak{m}$ are in direct correspondence to the solutions of

$$x^q - x = 0, \qquad \text{where } q = |k| = p^n.$$

These solutions are the Teichmüller representatives in K.

Elements in a Finite Unramified Extension of $\mathbb{Q}_p$

Theorem

For a finite unramified extension K of $\mathbb{Q}_p$, we can write any $x \in K$ **uniquely** as:

$$x = \sum_{k=m}^{\infty} a_k p^k,$$

for some $m \in \mathbb{Z}$ and where the a_k's are Teichmüller representatives.

Table of Contents

Krasner's Lemma

If $\alpha, \beta \in \overline{\mathbb{Q}}_p$ and β is chosen closer to α than any Galois conjugates of α, then

$$\mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta).$$

Theorem ("Nearby" Polynomials Define the Same Extensions)

Let $K/\mathbb{Q}_p$ be a finite extension. Let α have minimal polynomial $f(x) \in K[x]$. Then for monic $g(x) \in K[x]$ with "nearby" coefficients and β a root of $g(x)$. Then

$$K(\alpha) = K(\beta).$$

Note: we can replace K with $\mathbb{C}_p$.

Table of Contents

The Algebraic Closure of $\mathbb{Q}_p$ is Not Complete

Theorem

$\overline{\mathbb{Q}}_p$ is not complete.

Sketch of Proof

Consider the sequence

$$\beta_n = \sum_{i=0}^{n} \alpha_i p^{N_i}$$

with carefully chosen **Teichmüller representatives** α_n and increasing integers N_i.

We can make it so that the sequence has the property $\mathbb{Q}_p(\beta_n) \subset \mathbb{Q}_p(\beta)$, where $\beta := \sum_{i=0}^{\infty} \alpha_i p^{N_i}$.

The Completion of $\overline{\mathbb{Q}}_p$ is Algebraically Closed

Definition

We denote the completion of $\overline{\mathbb{Q}}_p$ as $\mathbb{C}_p$.

Theorem

$\mathbb{C}_p$ is algebraically closed, i.e. every non-constant polynomial in $\mathbb{C}_p[x]$ has a root in $\mathbb{C}_p$.

Sketch of Proof

Use:

- $\overline{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$
- Any root of $g(x) \in \overline{\mathbb{Q}}_p[x]$ has all its roots in $\overline{\mathbb{Q}}_p$
- *"Nearby" Polynomials Define the Same Extensions*

Table of Contents

Conclusion and Further Study

- Transcendence Degree
- $\mathbb{C}_p^{\text{unram}}/\mathbb{Q}_p$ has transcendence degree $2^{\aleph_0} = |\mathbb{R}|$.
- $\mathbb{C}_p/\mathbb{C}_p^{\text{unram}}$ has transcendence degree $2^{\aleph_0}$.

Any Questions?