Demystifying the p-adics

an invitation to the non-Archimedean world

Deewang Bhamidipati

6th November 2020

Why care about $\mathbb{Q}_p$?

Why care about $\mathbb{Q}_p$?

Here are a few incomplete and imperfect answers

Why care about $\mathbb{Q}_p$?

Here are a few incomplete and imperfect answers

- They're the other metric completions of $\mathbb{Q}$, so why not spend time understanding them given how much we understand $\mathbb{R}$.

Why care about $\mathbb{Q}_p$?

Here are a few incomplete and imperfect answers

- They're the other metric completions of $\mathbb{Q}$, so why not spend time understanding them given how much we understand $\mathbb{R}$.
- They are a bridge between the characteristic 0 and characteristic p world.

Why care about $\mathbb{Q}_p$?

Here are a few incomplete and imperfect answers

- They're the other metric completions of $\mathbb{Q}$, so why not spend time understanding them given how much we understand $\mathbb{R}$.
- They are a bridge between the characteristic 0 and characteristic p world.
- They're the building blocks of the "adelic perspective", a perspective core to Class Field Theory and candidates for non-abelian Class Field Theory like the Langlands program, and Iwasawa Theory, for example.

Why care about $\mathbb{Q}_p$?

Here are a few incomplete and imperfect answers

- They're the other metric completions of $\mathbb{Q}$, so why not spend time understanding them given how much we understand $\mathbb{R}$.
- They are a bridge between the characteristic 0 and characteristic p world.
- They're the building blocks of the "adelic perspective", a perspective core to Class Field Theory and candidates for non-abelian Class Field Theory like the Langlands program, and Iwasawa Theory, for example.
- Historically, and perhaps surprisingly, p-adic theory yielded a proof of the first of the Weil Conjectures, the question on rationality of the concerned zeta function, by Dwork.

Why care about $\mathbb{Q}_p$?

Here are a few incomplete and imperfect answers

- They're the other metric completions of $\mathbb{Q}$, so why not spend time understanding them given how much we understand $\mathbb{R}$.
- They are a bridge between the characteristic 0 and characteristic p world.
- They're the building blocks of the "adelic perspective", a perspective core to Class Field Theory and candidates for non-abelian Class Field Theory like the Langlands program, and Iwasawa Theory, for example.
- Historically, and perhaps surprisingly, p-adic theory yielded a proof of the first of the Weil Conjectures, the question on rationality of the concerned zeta function, by Dwork.
- Their weirdness just makes them very fun!

What will we start answering?

the questions, in no particular order

What will we start answering?

the questions, in no particular order

- What are they?

What will we start answering?

the questions, in no particular order

- What are they?
- What do we know about their topology?

What will we start answering?

the questions, in no particular order

- What are they?
- What do we know about their topology?
- What is their connection to the characteristic p-world?

What will we start answering?

the questions, in no particular order

- What are they?
- What do we know about their topology?
- What is their connection to the characteristic p-world?
- What does algebra and analysis of $\mathbb{Q}_p$ look like?

What will we start answering?

the questions, in no particular order

- What are they?
- What do we know about their topology?
- What is their connection to the characteristic p-world?
- What does algebra and analysis of $\mathbb{Q}_p$ look like?

and other miscellaneous things...

The p-adic Norm: a non-standard absolute value

The p-adic Norm: a non-standard absolute value

Let's fix a prime number p, and consider any rational number $r \in \mathbb{Q}$, then we can write

$$r = p^k \frac{m}{n}$$

for some $k \in \mathbb{Z}$, such that $p \nmid m, n$.

The p-adic Norm: a non-standard absolute value

Let's fix a prime number p, and consider any rational number $r \in \mathbb{Q}$, then we can write

$$r = p^k \frac{m}{n}$$

for some $k \in \mathbb{Z}$, such that $p \nmid m, n$.

the p-adic norm

The p-adic Norm: a non-standard absolute value

Let's fix a prime number p, and consider any rational number $r \in \mathbb{Q}$, then we can write

$$r = p^k \frac{m}{n}$$

for some $k \in \mathbb{Z}$, such that $p \nmid m, n$.

the p-adic norm

Define

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$$

as

$$|r|_p = \left| p^k \frac{m}{n} \right|_p \coloneqq p^{-k} \quad \text{and} \quad |0|_p \coloneqq 0$$

The p-adic Norm: a non-standard absolute value

Let's fix a prime number p, and consider any rational number $r \in \mathbb{Q}$, then we can write

$$r = p^k \frac{m}{n}$$

for some $k \in \mathbb{Z}$, such that $p \nmid m, n$.

the p-adic norm

Define

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$$

as

$$|r|_p = \left| p^k \frac{m}{n} \right|_p := p^{-k} \quad \text{and} \quad |0|_p := 0$$

The p-adic norm satisfies the *strong triangle inequality*

$$|r + s|_p \leq \max\{|r|_p, |s|_p\}, \quad \text{for any } r, s \in \mathbb{Q}$$

This inequality implies the regular triangle inequality

We call such a norm *non-Archimedean*.

The p-adic Norm: non-Archimedean

Recall the Archimedean property from the last time you saw real analysis

The p-adic Norm: non-Archimedean

Recall the Archimedean property from the last time you saw real analysis

Archimedean property

The natural numbers are not bounded, i.e.,

$$\text{for any } M \in \mathbb{Q}, \text{ there exists an } n \in \mathbb{N} \text{ such that } |n|_\infty = n > M$$

Recall the Archimedean property from the last time you saw real analysis

Archimedean property

The natural numbers are not bounded, i.e.,

$$\text{for any } M \in \mathbb{Q}, \text{ there exists an } n \in \mathbb{N} \text{ such that } |n|_\infty = n > M$$

So we say $|\cdot|_\infty$ is Archimedean.

Recall the Archimedean property from the last time you saw real analysis

Archimedean property

The natural numbers are not bounded, i.e.,

$$\text{for any } M \in \mathbb{Q}, \text{ there exists an } n \in \mathbb{N} \text{ such that } |n|_\infty = n > M$$

So we say $|\cdot|_\infty$ is Archimedean.

Why is $|\cdot|_p$ called non-Archimedean?

Recall the Archimedean property from the last time you saw real analysis

Archimedean property

The natural numbers are not bounded, i.e.,

$$\text{for any } M \in \mathbb{Q}, \text{ there exists an } n \in \mathbb{N} \text{ such that } |n|_\infty = n > M$$

So we say $|\cdot|_\infty$ is Archimedean.

Why is $|\cdot|_p$ called non-Archimedean?

The natural numbers are **bounded** with respect to $|\cdot|_p$

$$|n|_p = |1 + \cdots + 1|_p \leq \max\{|1|_p, \ldots, |1|_p\} = |1|_p = 1$$

for any $n \in \mathbb{N}$.

The p-adic Norm: ultrametric

The p-adic Norm: ultrametric

We can now define a metric from our p-adic norm

We can now define a metric from our p-adic norm

the p-adic metric

We define, for any $r, s \in \mathbb{Q}$

$$d_p(r, s) \coloneqq |r - s|_p$$

A metric induced by a non-Archimedean norm is called an *ultrametric*.

We can now define a metric from our p-adic norm

the p-adic metric

We define, for any $r, s \in \mathbb{Q}$

$$d_p(r, s) := |r - s|_p$$

A metric induced by a non-Archimedean norm is called an *ultrametric*.

Therefore the strong triangle inequality

$$d_p(r, s) \leq \max\{d_p(r, t), d_p(t, s)\}$$

is also called the *ultrametric inequality*.

Towards $\mathbb{Q}_p$: why $\mathbb{R}$?

Towards $\mathbb{Q}_p$: why $\mathbb{R}$?

We're missing irrational numbers!

Towards $\mathbb{Q}_p$: why $\mathbb{R}$?

We're missing irrational numbers! More technically put, there are rational Cauchy sequences (with respect to $|\cdot|_\infty$) that don't converges in $\mathbb{Q}$.

Towards $\mathbb{Q}_p$: why $\mathbb{R}$?

We're missing irrational numbers! More technically put, there are rational Cauchy sequences (with respect to $|\cdot|_\infty$) that don't converges in $\mathbb{Q}$. For example,

$$a_0 = 1, \quad a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right)$$

is a Cauchy sequence of rationals such that $a_n^2 \to 2$.

Construction of $(\mathbb{R}, |\cdot|_\infty)$, i.e., completing $(\mathbb{Q}, |\cdot|_\infty)$

We're missing irrational numbers! More technically put, there are rational Cauchy sequences (with respect to $|\cdot|_\infty$) that don't converges in $\mathbb{Q}$. For example,

$$a_0 = 1, \quad a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right)$$

is a Cauchy sequence of rationals such that $a_n^2 \to 2$.

Construction of $(\mathbb{R}, |\cdot|_\infty)$, i.e., completing $(\mathbb{Q}, |\cdot|_\infty)$

This set

$$C_s = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_\infty\}$$

is a ring with pointwise addition and multiplication,

Towards $\mathbb{Q}_p$: why $\mathbb{R}$?

We're missing irrational numbers! More technically put, there are rational Cauchy sequences (with respect to $|\cdot|_\infty$) that don't converges in $\mathbb{Q}$. For example,

$$a_0 = 1, \quad a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right)$$

is a Cauchy sequence of rationals such that $a_n^2 \to 2$.

Construction of $(\mathbb{R}, |\cdot|_\infty)$, i.e., completing $(\mathbb{Q}, |\cdot|_\infty)$

This set

$$C_s = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_\infty\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_s = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_\infty\} \subseteq C_s$$

Towards $\mathbb{Q}_p$: why $\mathbb{R}$?

We're missing irrational numbers! More technically put, there are rational Cauchy sequences (with respect to $|\cdot|_\infty$) that don't converges in $\mathbb{Q}$. For example,

$$a_0 = 1, \quad a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right)$$

is a Cauchy sequence of rationals such that $a_n^2 \to 2$.

Construction of $(\mathbb{R}, |\cdot|_\infty)$, i.e., completing $(\mathbb{Q}, |\cdot|_\infty)$

This set

$$C_s = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_\infty\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_s = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_\infty\} \subseteq C_s$$

a maximal ideal of C_s.

Towards $\mathbb{Q}_p$: why $\mathbb{R}$?

We're missing irrational numbers! More technically put, there are rational Cauchy sequences (with respect to $|\cdot|_\infty$) that don't converges in $\mathbb{Q}$. For example,

$$a_0 = 1, \quad a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right)$$

is a Cauchy sequence of rationals such that $a_n^2 \to 2$.

Construction of $(\mathbb{R}, |\cdot|_\infty)$, i.e., completing $(\mathbb{Q}, |\cdot|_\infty)$

This set

$$C_s = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_\infty\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_s = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_\infty\} \subseteq C_s$$

a maximal ideal of C_s. So, $\mathbb{R} \coloneqq C_s/M_s$, and $|\cdot|_\infty$ lifts.

Towards $\mathbb{Q}_p$: why $\mathbb{R}$?

We're missing irrational numbers! More technically put, there are rational Cauchy sequences (with respect to $|\cdot|_\infty$) that don't converges in $\mathbb{Q}$. For example,

$$a_0 = 1, \quad a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right)$$

is a Cauchy sequence of rationals such that $a_n^2 \to 2$.

Construction of $(\mathbb{R}, |\cdot|_\infty)$, i.e., completing $(\mathbb{Q}, |\cdot|_\infty)$

This set

$$C_s = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_\infty\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_s = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_\infty\} \subseteq C_s$$

a maximal ideal of C_s. So, $\mathbb{R} \coloneqq C_s/M_s$, and $|\cdot|_\infty$ lifts.

Yes, $(\mathbb{Q}_p, |\cdot|_p)$ is the completion of the normed space $(\mathbb{Q}, |\cdot|_p)$.

Towards $\mathbb{Q}_p$: $(\mathbb{Q}, |\cdot|_p)$ incomplete?

Towards $\mathbb{Q}_p$: $(\mathbb{Q}, |\cdot|_p)$ incomplete?

For $p = 7$, consider the following modular congruence for any $n \in \mathbb{N}$

$$x^2 \equiv 2 \bmod 7^n$$

Towards $\mathbb{Q}_p$: $(\mathbb{Q}, |\cdot|_p)$ incomplete?

For $p = 7$, consider the following modular congruence for any $n \in \mathbb{N}$

$$x^2 \equiv 2 \bmod 7^n$$

- For $n = 1$, we have the solution $x \equiv \pm 3 \bmod 7$, let $x_1 \coloneqq 3$.

Towards $\mathbb{Q}_p$: $(\mathbb{Q}, |\cdot|_p)$ incomplete?

For $p = 7$, consider the following modular congruence for any $n \in \mathbb{N}$

$$x^2 \equiv 2 \bmod 7^n$$

- For $n = 1$, we have the solution $x \equiv \pm 3 \bmod 7$, let $x_1 \coloneqq 3$.
- For $n = 2$, any solution mod 7^2 is necessarily also a solution mod 7. So, let $x_2 \coloneqq x_1 + 7y = 3 + 7y$; solving the equation for y, you get $y \equiv 1 \bmod 7$. Therefore, we let $x_2 = 3 + 1 \cdot 7 = 10$.

Towards $\mathbb{Q}_p$: $(\mathbb{Q}, |\cdot|_p)$ incomplete?

For $p = 7$, consider the following modular congruence for any $n \in \mathbb{N}$

$$x^2 \equiv 2 \bmod 7^n$$

- For $n = 1$, we have the solution $x \equiv \pm 3 \bmod 7$, let $x_1 \coloneqq 3$.
- For $n = 2$, any solution mod 7^2 is necessarily also a solution mod 7. So, let $x_2 \coloneqq x_1 + 7y = 3 + 7y$; solving the equation for y, you get $y \equiv 1 \bmod 7$. Therefore, we let $x_2 = 3 + 1 \cdot 7 = 10$.
- For $n = 3$, any solution mod 7^3 is necessarily also a solution mod 7^2. So, let $x_3 \coloneqq x_2 + 7^2 y = 3 + 1 \cdot 7 + 7^2 y$; solving the equation for y, you get $y \equiv 2 \bmod 7$. Therefore, we let $x_3 = 3 + 1 \cdot 7 + 2 \cdot 7^2 = 108$.

Towards $\mathbb{Q}_p$: $(\mathbb{Q}, |\cdot|_p)$ incomplete?

For $p = 7$, consider the following modular congruence for any $n \in \mathbb{N}$

$$x^2 \equiv 2 \bmod 7^n$$

- For $n = 1$, we have the solution $x \equiv \pm 3 \bmod 7$, let $x_1 \coloneqq 3$.
- For $n = 2$, any solution mod 7^2 is necessarily also a solution mod 7. So, let $x_2 \coloneqq x_1 + 7y = 3 + 7y$; solving the equation for y, you get $y \equiv 1 \bmod 7$. Therefore, we let $x_2 = 3 + 1 \cdot 7 = 10$.
- For $n = 3$, any solution mod 7^3 is necessarily also a solution mod 7^2. So, let $x_3 \coloneqq x_2 + 7^2 y = 3 + 1 \cdot 7 + 7^2 y$; solving the equation for y, you get $y \equiv 2 \bmod 7$. Therefore, we let $x_3 = 3 + 1 \cdot 7 + 2 \cdot 7^2 = 108$.
- Continuing similarly, $x_4 = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 = 2166$.

Towards $\mathbb{Q}_p$: $(\mathbb{Q}, |\cdot|_p)$ incomplete?

For $p = 7$, consider the following modular congruence for any $n \in \mathbb{N}$

$$x^2 \equiv 2 \bmod 7^n$$

- For $n = 1$, we have the solution $x \equiv \pm 3 \bmod 7$, let $x_1 := 3$.
- For $n = 2$, any solution mod 7^2 is necessarily also a solution mod 7. So, let $x_2 := x_1 + 7y = 3 + 7y$; solving the equation for y, you get $y \equiv 1 \bmod 7$. Therefore, we let $x_2 = 3 + 1 \cdot 7 = 10$.
- For $n = 3$, any solution mod 7^3 is necessarily also a solution mod 7^2. So, let $x_3 := x_2 + 7^2 y = 3 + 1 \cdot 7 + 7^2 y$; solving the equation for y, you get $y \equiv 2 \bmod 7$. Therefore, we let $x_3 = 3 + 1 \cdot 7 + 2 \cdot 7^2 = 108$.
- Continuing similarly, $x_4 = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 = 2166$.

Iteratively, we have define a sequence of rationals (x_n), where

$$x_{n+1}^2 \equiv x_n^2 + x_n - 2 \bmod 7^{n+1} \quad \text{and} \quad x_n^2 \equiv 2 \bmod 7^n$$

Towards $\mathbb{Q}_p$: $(\mathbb{Q}, |\cdot|_p)$ incomplete?

For $p = 7$, consider the following modular congruence for any $n \in \mathbb{N}$

$$x^2 \equiv 2 \bmod 7^n$$

- For $n = 1$, we have the solution $x \equiv \pm 3 \bmod 7$, let $x_1 \coloneqq 3$.
- For $n = 2$, any solution mod 7^2 is necessarily also a solution mod 7. So, let $x_2 \coloneqq x_1 + 7y = 3 + 7y$; solving the equation for y, you get $y \equiv 1 \bmod 7$. Therefore, we let $x_2 = 3 + 1 \cdot 7 = 10$.
- For $n = 3$, any solution mod 7^3 is necessarily also a solution mod 7^2. So, let $x_3 \coloneqq x_2 + 7^2 y = 3 + 1 \cdot 7 + 7^2 y$; solving the equation for y, you get $y \equiv 2 \bmod 7$. Therefore, we let $x_3 = 3 + 1 \cdot 7 + 2 \cdot 7^2 = 108$.
- Continuing similarly, $x_4 = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 = 2166$.

Iteratively, we have define a sequence of rationals (x_n), where

$$x_{n+1}^2 \equiv x_n^2 + x_n - 2 \bmod 7^{n+1} \quad \text{and} \quad x_n^2 \equiv 2 \bmod 7^n$$

This is a Cauchy sequence with respect to the 7-adic norm, and it clearly doesn't converges in $\mathbb{Q}$.

For $p = 7$, consider the following modular congruence for any $n \in \mathbb{N}$

$$x^2 \equiv 2 \bmod 7^n$$

- For $n = 1$, we have the solution $x \equiv \pm 3 \bmod 7$, let $x_1 := 3$.
- For $n = 2$, any solution mod 7^2 is necessarily also a solution mod 7. So, let $x_2 := x_1 + 7y = 3 + 7y$; solving the equation for y, you get $y \equiv 1 \bmod 7$. Therefore, we let $x_2 = 3 + 1 \cdot 7 = 10$.
- For $n = 3$, any solution mod 7^3 is necessarily also a solution mod 7^2. So, let $x_3 := x_2 + 7^2 y = 3 + 1 \cdot 7 + 7^2 y$; solving the equation for y, you get $y \equiv 2 \bmod 7$. Therefore, we let $x_3 = 3 + 1 \cdot 7 + 2 \cdot 7^2 = 108$.
- Continuing similarly, $x_4 = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 = 2166$.

Iteratively, we have define a sequence of rationals (x_n), where

$$x_{n+1}^2 \equiv x_n^2 + x_n - 2 \bmod 7^{n+1} \quad \text{and} \quad x_n^2 \equiv 2 \bmod 7^n$$

This is a Cauchy sequence with respect to the 7-adic norm, and it clearly doesn't converges in $\mathbb{Q}$. Because if it did, that would be a rational number $x \in \mathbb{Q}$ such that $x^2 \equiv 2 \bmod 7^n$, for every $n \in \mathbb{N}$.

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Construction of $(\mathbb{Q}_p, |\cdot|_p)$, i.e., completing $(\mathbb{Q}, |\cdot|_p)$

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Construction of $(\mathbb{Q}_p, |\cdot|_p)$, i.e., completing $(\mathbb{Q}, |\cdot|_p)$

This set

$$C_p = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_p\}$$

is a ring with pointwise addition and multiplication,

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Construction of $(\mathbb{Q}_p, |\cdot|_p)$, i.e., completing $(\mathbb{Q}, |\cdot|_p)$

This set

$$C_p = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_p\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_p = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_p\} \subseteq C_p$$

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Construction of $(\mathbb{Q}_p, |\cdot|_p)$, i.e., completing $(\mathbb{Q}, |\cdot|_p)$

This set

$$C_p = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_p\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_p = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_p\} \subseteq C_p$$

a maximal ideal of C_p.

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Construction of $(\mathbb{Q}_p, |\cdot|_p)$, i.e., completing $(\mathbb{Q}, |\cdot|_p)$

This set

$$C_p = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_p\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_p = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_p\} \subseteq C_p$$

a maximal ideal of C_p. So, $\mathbb{Q}_p \coloneqq C_p/M_p$, and $|\cdot|_p$ lifts.

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Construction of $(\mathbb{Q}_p, |\cdot|_p)$, i.e., completing $(\mathbb{Q}, |\cdot|_p)$

This set

$$C_p = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_p\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_p = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_p\} \subseteq C_p$$

a maximal ideal of C_p. So, $\mathbb{Q}_p \coloneqq C_p/M_p$, and $|\cdot|_p$ lifts.

$\mathbb{Z}_p$, the analogue of $[-1, 1]$

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Construction of $(\mathbb{Q}_p, |\cdot|_p)$, i.e., completing $(\mathbb{Q}, |\cdot|_p)$

This set

$$C_p = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_p\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_p = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_p\} \subseteq C_p$$

a maximal ideal of C_p. So, $\mathbb{Q}_p \coloneqq C_p / M_p$, and $|\cdot|_p$ lifts.

$\mathbb{Z}_p$, the analogue of $[-1, 1]$

We define

$$\mathbb{Z}_p \coloneqq \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Construction of $(\mathbb{Q}_p, |\cdot|_p)$, i.e., completing $(\mathbb{Q}, |\cdot|_p)$

This set

$$C_p = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_p\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_p = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_p\} \subseteq C_p$$

a maximal ideal of C_p. So, $\mathbb{Q}_p \coloneqq C_p/M_p$, and $|\cdot|_p$ lifts.

$\mathbb{Z}_p$, the analogue of $[-1, 1]$

We define

$$\mathbb{Z}_p \coloneqq \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

It is a local ring, with the unique maximal ideal (the interior)

$$p\mathbb{Z}_p \coloneqq \{x \in \mathbb{Q}_p \mid |x|_p < 1\}$$

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Construction of $(\mathbb{Q}_p, |\cdot|_p)$, i.e., completing $(\mathbb{Q}, |\cdot|_p)$

This set

$$C_p = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_p\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_p = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_p\} \subseteq C_p$$

a maximal ideal of C_p. So, $\mathbb{Q}_p \coloneqq C_p/M_p$, and $|\cdot|_p$ lifts.

$\mathbb{Z}_p$, the analogue of $[-1, 1]$

We define

$$\mathbb{Z}_p \coloneqq \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

It is a local ring, with the unique maximal ideal (the interior)

$$p\mathbb{Z}_p \coloneqq \{x \in \mathbb{Q}_p \mid |x|_p < 1\}$$

and residue field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$

Constructing $\mathbb{Q}_p$: construction I & $\mathbb{Z}_p$

Construction of $(\mathbb{Q}_p, |\cdot|_p)$, i.e., completing $(\mathbb{Q}, |\cdot|_p)$

This set

$$C_p = \{(a_n) \mid (a_n) \text{ is Cauchy with respect to } |\cdot|_p\}$$

is a ring with pointwise addition and multiplication, and the following set of null sequences

$$M_p = \{(a_n) \mid a_n \to 0 \text{ with respect to } |\cdot|_p\} \subseteq C_p$$

a maximal ideal of C_p. So, $\mathbb{Q}_p \coloneqq C_p/M_p$, and $|\cdot|_p$ lifts.

$\mathbb{Z}_p$, the analogue of $[-1, 1]$

We define

$$\mathbb{Z}_p \coloneqq \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

It is a local ring, with the unique maximal ideal (the interior)

$$p\mathbb{Z}_p \coloneqq \{x \in \mathbb{Q}_p \mid |x|_p < 1\}$$

and residue field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$, and group of units (the boundary)

$$\mathbb{Z}_p^\times \coloneqq \{x \in \mathbb{Q}_p \mid |x|_p = 1\}$$

Ostrowski's theorem classification of completions of $\mathbb{Q}$

Two metrics are said to be equivalent if they induce the same topology, and two norms are said to be equivalent if their induced metrics are equivalent.

Two metrics are said to be equivalent if they induce the same topology, and two norms are said to be equivalent if their induced metrics are equivalent.

the trivial norm

For any field k, we can define the trivial norm

$$|x|_* := \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$$

Two metrics are said to be equivalent if they induce the same topology, and two norms are said to be equivalent if their induced metrics are equivalent.

the trivial norm

For any field k, we can define the trivial norm

$$|x|_* := \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$$

Theorem (Ostrowski, 1918)

Ostrowski's theorem classification of completions of $\mathbb{Q}$

Two metrics are said to be equivalent if they induce the same topology, and two norms are said to be equivalent if their induced metrics are equivalent.

the trivial norm

For any field k, we can define the trivial norm

$$|x|_* := \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$$

Theorem (Ostrowski, 1918)

Every non-trivial norm $\|\cdot\|$ on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p or $|\cdot|_\infty$, the standard absolute value.

Two metrics are said to be equivalent if they induce the same topology, and two norms are said to be equivalent if their induced metrics are equivalent.

the trivial norm

For any field k, we can define the trivial norm

$$|x|_* := \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$$

Theorem (Ostrowski, 1918)

Every non-trivial norm $\|\cdot\|$ on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p or $|\cdot|_\infty$, the standard absolute value.

So, the only completions of $\mathbb{Q}$ are $\mathbb{Q}$ (with respect to the trivial norm), $\mathbb{R}$ and $\mathbb{Q}_p$, for any prime p.

Constructing $\mathbb{Q}_p$: construction II, 1

The completion construction is a bit opaque. We construct $\mathbb{Q}_p$ more algebraically.

The completion construction is a bit opaque. We construct $\mathbb{Q}_p$ more algebraically.

The ring $\mathbb{Z}/p^n\mathbb{Z}$

Any element of the ring $\mathbb{Z}/p^n\mathbb{Z}$ can be unique written as

$$a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$$

for some a_i lying between 0 and $p-1$, for any $i = 0, \ldots, n-1$

Constructing $\mathbb{Q}_p$: construction II, 1

The completion construction is a bit opaque. We construct $\mathbb{Q}_p$ more algebraically.

The ring $\mathbb{Z}/p^n\mathbb{Z}$

Any element of the ring $\mathbb{Z}/p^n\mathbb{Z}$ can be unique written as

$$a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$$

for some a_i lying between 0 and $p-1$, for any $i = 0, \ldots, n-1$

Constructing $\mathbb{Z}_p$

Constructing $\mathbb{Q}_p$: construction II, 1

The completion construction is a bit opaque. We construct $\mathbb{Q}_p$ more algebraically.

The ring $\mathbb{Z}/p^n\mathbb{Z}$

Any element of the ring $\mathbb{Z}/p^n\mathbb{Z}$ can be unique written as

$$a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$$

for some a_i lying between 0 and $p-1$, for any $i = 0, \ldots, n-1$

Constructing $\mathbb{Z}_p$

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

where system consists of the natural projections of reductions $\pi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$.

Constructing $\mathbb{Q}_p$: construction II, 1

The completion construction is a bit opaque. We construct $\mathbb{Q}_p$ more algebraically.

The ring $\mathbb{Z}/p^n\mathbb{Z}$

Any element of the ring $\mathbb{Z}/p^n\mathbb{Z}$ can be unique written as

$$a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$$

for some a_i lying between 0 and $p-1$, for any $i = 0, \ldots, n-1$

Constructing $\mathbb{Z}_p$

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

where system consists of the natural projections of reductions $\pi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$.
We now have a very good description of the ring $\mathbb{Z}_p$, an integral domain

$$\mathbb{Z}_p = \left\{ \sum_{n \geq 0} a_n p^n \,\middle|\, 0 \leq a_n \leq p-1, \ \forall n \right\}$$

Constructing $\mathbb{Q}_p$: construction II, 1

The completion construction is a bit opaque. We construct $\mathbb{Q}_p$ more algebraically.

The ring $\mathbb{Z}/p^n\mathbb{Z}$

Any element of the ring $\mathbb{Z}/p^n\mathbb{Z}$ can be unique written as

$$a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$$

for some a_i lying between 0 and $p-1$, for any $i = 0, \ldots, n-1$

Constructing $\mathbb{Z}_p$

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

where system consists of the natural projections of reductions $\pi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$. We now have a very good description of the ring $\mathbb{Z}_p$, an integral domain

$$\mathbb{Z}_p = \left\{ \sum_{n \geq 0} a_n p^n \;\middle|\; 0 \leq a_n \leq p-1, \ \forall n \right\}$$

Think Taylor series/holomorphic functions. Let the coefficients of the “Taylor expansion" of any $x \in \mathbb{Z}_p$ notationally be $a_n(x)$.

Constructing $\mathbb{Q}_p$: construction II, 2

Constructing $\mathbb{Q}_p$: construction II, 2

p-adic norm on $\mathbb{Z}_p$

Any $x \in \mathbb{Z}_p$ can be uniquely written as $x = p^n u$, for some $n \geq 0$, such that $a_0(u) \neq 0$. We define

$$|x|_p \coloneqq p^{-n}$$

We can now define the p-adic metric via this p-adic norm.

Constructing $\mathbb{Q}_p$: construction II, 2

p-adic norm on $\mathbb{Z}_p$

Any $x \in \mathbb{Z}_p$ can be uniquely written as $x = p^n u$, for some $n \geq 0$, such that $a_0(u) \neq 0$. We define

$$|x|_p \coloneqq p^{-n}$$

We can now define the p-adic metric via this p-adic norm.

the metric space $(\mathbb{Z}_p, |\cdot|_p)$

Constructing $\mathbb{Q}_p$: construction II, 2

p-adic norm on $\mathbb{Z}_p$

Any $x \in \mathbb{Z}_p$ can be uniquely written as $x = p^n u$, for some $n \geq 0$, such that $a_0(u) \neq 0$. We define

$$|x|_p \coloneqq p^{-n}$$

We can now define the p-adic metric via this p-adic norm.

the metric space $(\mathbb{Z}_p, |\cdot|_p)$

$\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

Constructing $\mathbb{Q}_p$: construction II, 2

p-adic norm on $\mathbb{Z}_p$

Any $x \in \mathbb{Z}_p$ can be uniquely written as $x = p^n u$, for some $n \geq 0$, such that $a_0(u) \neq 0$. We define

$$|x|_p := p^{-n}$$

We can now define the p-adic metric via this p-adic norm.

the metric space $(\mathbb{Z}_p, |\cdot|_p)$

$\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

the field $\mathbb{Q}_p$

Constructing $\mathbb{Q}_p$: construction II, 2

p-adic norm on $\mathbb{Z}_p$

Any $x \in \mathbb{Z}_p$ can be uniquely written as $x = p^n u$, for some $n \geq 0$, such that $a_0(u) \neq 0$. We define

$$|x|_p := p^{-n}$$

We can now define the p-adic metric via this p-adic norm.

the metric space $(\mathbb{Z}_p, |\cdot|_p)$

$\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

the field $\mathbb{Q}_p$

Think Laurent series/meromorphic functions

$$\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p) = \left\{ \sum_{n \geq -N} a_n p^n \;\middle|\; 0 \leq a_n \leq p-1, \ \forall n \right\}$$

$|\cdot|_p$ lifts, and $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

is open

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

is open (and closed from what follows below)!

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

is open (and closed from what follows below)!

open balls

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

is open (and closed from what follows below)!

open balls

The open balls

$$B(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^n\}$$

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x-a|_p = p^n\}$$

is open (and closed from what follows below)!

open balls

The open balls

$$B(a, p^n) = \{x \in \mathbb{Q}_p \mid |x-a|_p < p^n\}$$

are closed and open!

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

is open (and closed from what follows below)!

open balls

The open balls

$$B(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^n\}$$

are closed and open!

closed balls

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

is open (and closed from what follows below)!

open balls

The open balls

$$B(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^n\}$$

are closed and open!

closed balls

The closed balls

$$\overline{B}(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p \leq p^n\}$$

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

is open (and closed from what follows below)!

open balls

The open balls

$$B(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^n\}$$

are closed and open!

closed balls

The closed balls

$$\overline{B}(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p \leq p^n\} = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^{n+1}\}$$

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

is open (and closed from what follows below)!

open balls

The open balls

$$B(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^n\}$$

are closed and open!

closed balls

The closed balls

$$\overline{B}(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p \leq p^n\} = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^{n+1}\} = B(a, p^{n+1})$$

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

is open (and closed from what follows below)!

open balls

The open balls

$$B(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^n\}$$

are closed and open!

closed balls

The closed balls

$$\overline{B}(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p \leq p^n\} = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^{n+1}\} = B(a, p^{n+1})$$

are closed and open!

Metric topology of $\mathbb{Q}_p$: paradoxical properties

Note that unlike $|\cdot|_\infty$, the image of $|\cdot|_p$ is the discrete set $\{p^n \mid n \in \mathbb{Z}\}$.

the sphere

The "sphere"

$$S(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p = p^n\}$$

is open (and closed from what follows below)!

open balls

The open balls

$$B(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^n\}$$

are closed and open!

closed balls

The closed balls

$$\overline{B}(a, p^n) = \{x \in \mathbb{Q}_p \mid |x - a|_p \leq p^n\} = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^{n+1}\} = B(a, p^{n+1})$$

are closed and open!

Metric topology of $\mathbb{Q}_p$: more paradoxical properties

centers of balls

Metric topology of $\mathbb{Q}_p$: more paradoxical properties

centers of balls

For any $b \in B(a, r)$, we have $B(a, r) = B(b, r)$

Metric topology of $\mathbb{Q}_p$: more paradoxical properties

centers of balls

For any $b \in B(a, r)$, we have $B(a, r) = B(b, r)$, i.e. every point of a ball is its center!

Metric topology of $\mathbb{Q}_p$: more paradoxical properties

centers of balls

For any $b \in B(a, r)$, we have $B(a, r) = B(b, r)$, i.e. every point of a ball is its center!

intersections of open balls

Metric topology of $\mathbb{Q}_p$: more paradoxical properties

centers of balls

For any $b \in B(a, r)$, we have $B(a, r) = B(b, r)$, i.e. every point of a ball is its center!

intersections of open balls

$B(x, r) \cap B(y, s) \neq \emptyset$ if and only if $B(x, r) \subseteq B(y, s)$ or $B(y, s) \subseteq B(x, r)$

Metric topology of $\mathbb{Q}_p$: more paradoxical properties

centers of balls

For any $b \in B(a, r)$, we have $B(a, r) = B(b, r)$, i.e. every point of a ball is its center!

intersections of open balls

$B(x, r) \cap B(y, s) \neq \emptyset$ if and only if $B(x, r) \subseteq B(y, s)$ or $B(y, s) \subseteq B(x, r)$, i.e. two balls have a nonempty intersection if and only if one is contained in the other.

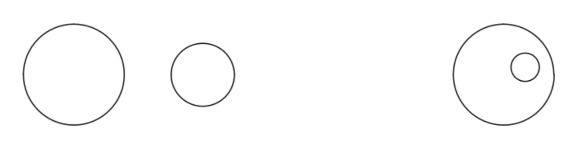
Metric topology of $\mathbb{Q}_p$: more paradoxical properties

centers of balls

For any $b \in B(a, r)$, we have $B(a, r) = B(b, r)$, i.e. every point of a ball is its center!

intersections of open balls

$B(x, r) \cap B(y, s) \neq \emptyset$ if and only if $B(x, r) \subseteq B(y, s)$ or $B(y, s) \subseteq B(x, r)$, i.e. two balls have a nonempty intersection if and only if one is contained in the other.



Metric topology of $\mathbb{Q}_p$: topological nature

Metric topology of $\mathbb{Q}_p$: topological nature

compactness

compactness

$\mathbb{Z}_p$ can be shown to be sequentially compact, i.e. for any p-adic integer, you can find a sequence of p-adic integers converging to it.

Metric topology of $\mathbb{Q}_p$: topological nature

compactness

$\mathbb{Z}_p$ can be shown to be sequentially compact, i.e. for any p-adic integer, you can find a sequence of p-adic integers converging to it.

Since we're in a metric space, we have $\mathbb{Z}_p$ is compact

Metric topology of $\mathbb{Q}_p$: topological nature

compactness

$\mathbb{Z}_p$ can be shown to be sequentially compact, i.e. for any p-adic integer, you can find a sequence of p-adic integers converging to it.

Since we're in a metric space, we have $\mathbb{Z}_p$ is compact, and therefore $\mathbb{Q}_p$ is locally compact.

Metric topology of $\mathbb{Q}_p$: topological nature

compactness

$\mathbb{Z}_p$ can be shown to be sequentially compact, i.e. for any p-adic integer, you can find a sequence of p-adic integers converging to it.

Since we're in a metric space, we have $\mathbb{Z}_p$ is compact, and therefore $\mathbb{Q}_p$ is locally compact.

connectedness and hausdorff

Metric topology of $\mathbb{Q}_p$: topological nature

compactness

$\mathbb{Z}_p$ can be shown to be sequentially compact, i.e. for any p-adic integer, you can find a sequence of p-adic integers converging to it.

Since we're in a metric space, we have $\mathbb{Z}_p$ is compact, and therefore $\mathbb{Q}_p$ is locally compact.

connectedness and hausdorff

Since $\mathbb{Q}_p$ is a metric space, it's Hausdorff.

Metric topology of $\mathbb{Q}_p$: topological nature

compactness

$\mathbb{Z}_p$ can be shown to be sequentially compact, i.e. for any p-adic integer, you can find a sequence of p-adic integers converging to it.

Since we're in a metric space, we have $\mathbb{Z}_p$ is compact, and therefore $\mathbb{Q}_p$ is locally compact.

connectedness and hausdorff

Since $\mathbb{Q}_p$ is a metric space, it's Hausdorff.

$\mathbb{Q}_p$ is totally disconnected

Metric topology of $\mathbb{Q}_p$: topological nature

compactness

$\mathbb{Z}_p$ can be shown to be sequentially compact, i.e. for any p-adic integer, you can find a sequence of p-adic integers converging to it.

Since we're in a metric space, we have $\mathbb{Z}_p$ is compact, and therefore $\mathbb{Q}_p$ is locally compact.

connectedness and hausdorff

Since $\mathbb{Q}_p$ is a metric space, it's Hausdorff.

$\mathbb{Q}_p$ is totally disconnected, i.e. the connected sets in $\mathbb{Q}_p$ are singletons and the empty set.

Metric topology of $\mathbb{Q}_p$: $\mathbb{Z}_p$

Metric topology of $\mathbb{Q}_p$: $\mathbb{Z}_p$

$\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$

Metric topology of $\mathbb{Q}_p$: $\mathbb{Z}_p$

$\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$

We have

$$\mathbb{Z}_p = \overline{B}(0, 1) = B(0, p)$$

So $\mathbb{Z}_p$ is open and closed.

Metric topology of $\mathbb{Q}_p$: $\mathbb{Z}_p$

$\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$

We have

$$\mathbb{Z}_p = \overline{B}(0,1) = B(0,p)$$

So $\mathbb{Z}_p$ is open and closed.We have

$$\mathbb{Z}_p^\times = S(0,1)$$

Metric topology of $\mathbb{Q}_p$: $\mathbb{Z}_p$

$\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$

We have

$$\mathbb{Z}_p = \overline{\mathrm{B}}(0,1) = \mathrm{B}(0,\mathrm{p})$$

So $\mathbb{Z}_p$ is open and closed.We have

$$\mathbb{Z}_p^\times = S(0,1) = (1 + p\mathbb{Z}_p) \cup (2 + p\mathbb{Z}_p) \cup \cdots ((p-1) + p\mathbb{Z}_p)$$

$\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$

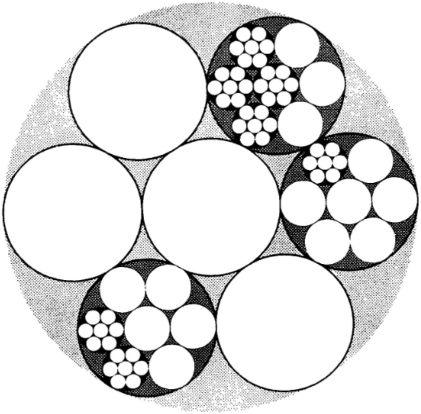
We have

$$\mathbb{Z}_p = \overline{B}(0,1) = B(0,p)$$

So $\mathbb{Z}_p$ is open and closed.We have

$$\mathbb{Z}_p^\times = S(0,1) = (1 + p\mathbb{Z}_p) \cup (2 + p\mathbb{Z}_p) \cup \cdots ((p-1) + p\mathbb{Z}_p)$$

Let's use this visualize $\mathbb{Z}_p$, for $p = 7$ and $p = 3$!



$\mathbb{Z}_7$

Artist's conception of the 3-adic unit disk.

Drawing by A.T. Fomenko of Moscow State University, Moscow, U.S.S.R.

Metric topology of $\mathbb{Q}_p$: Euclidean Models of $\mathbb{Z}_p$

Sets of $\mathbb{R}^n$ that are homeomorphic to $\mathbb{Z}_p$ are called Euclidean models.

Metric topology of $\mathbb{Q}_p$: Euclidean Models of $\mathbb{Z}_p$

Sets of $\mathbb{R}^n$ that are homeomorphic to $\mathbb{Z}_p$ are called Euclidean models.

one-dimensional

Sets of $\mathbb{R}^n$ that are homeomorphic to $\mathbb{Z}_p$ are called Euclidean models.

one-dimensional

The following map

$$\sum_{n=0}^{\infty} a_n 2^n \mapsto \sum_{n=0}^{\infty} \frac{2a_n}{3^{n+1}}$$

Metric topology of $\mathbb{Q}_p$: Euclidean Models of $\mathbb{Z}_p$

Sets of $\mathbb{R}^n$ that are homeomorphic to $\mathbb{Z}_p$ are called Euclidean models.

one-dimensional

The following map

$$\sum_{n=0}^{\infty} a_n 2^n \mapsto \sum_{n=0}^{\infty} \frac{2a_n}{3^{n+1}}$$

gives a homeomorphism between $\mathbb{Z}_2$ and the cantor set $\mathcal{C}$.

Sets of $\mathbb{R}^n$ that are homeomorphic to $\mathbb{Z}_p$ are called Euclidean models.

one-dimensional

The following map

$$\sum_{n=0}^{\infty} a_n 2^n \mapsto \sum_{n=0}^{\infty} \frac{2a_n}{3^{n+1}}$$

gives a homeomorphism between $\mathbb{Z}_2$ and the cantor set $\mathcal{C}$.

You can construct Cantor-like sets $\mathcal{C}^p$, where numbers can be written in base $2p-1$; starting with the unit interval, and continuing recursively, divide into $2p-1$ pieces and delete the second piece. Taking the intersection of the resulting pieces gives you $\mathcal{C}^p$.

Metric topology of $\mathbb{Q}_p$: Euclidean Models of $\mathbb{Z}_p$

Sets of $\mathbb{R}^n$ that are homeomorphic to $\mathbb{Z}_p$ are called Euclidean models.

one-dimensional

The following map

$$\sum_{n=0}^{\infty} a_n 2^n \mapsto \sum_{n=0}^{\infty} \frac{2a_n}{3^{n+1}}$$

gives a homeomorphism between $\mathbb{Z}_2$ and the cantor set $\mathcal{C}$.

You can construct Cantor-like sets $\mathcal{C}^p$, where numbers can be written in base $2p-1$; starting with the unit interval, and continuing recursively, divide into $2p-1$ pieces and delete the second piece. Taking the intersection of the resulting pieces gives you $\mathcal{C}^p$.The following map

$$\sum_{n=0}^{\infty} a_n p^n \mapsto \sum_{n=0}^{\infty} \frac{2a_n}{(2p-1)^{n+1}}$$

Sets of $\mathbb{R}^n$ that are homeomorphic to $\mathbb{Z}_p$ are called Euclidean models.

one-dimensional

The following map

$$\sum_{n=0}^{\infty} a_n 2^n \mapsto \sum_{n=0}^{\infty} \frac{2a_n}{3^{n+1}}$$

gives a homeomorphism between $\mathbb{Z}_2$ and the cantor set $\mathcal{C}$.

You can construct Cantor-like sets $\mathcal{C}^p$, where numbers can be written in base $2p-1$; starting with the unit interval, and continuing recursively, divide into $2p-1$ pieces and delete the second piece. Taking the intersection of the resulting pieces gives you $\mathcal{C}^p$.The following map

$$\sum_{n=0}^{\infty} a_n p^n \mapsto \sum_{n=0}^{\infty} \frac{2a_n}{(2p-1)^{n+1}}$$

gives a homeomorphism between $\mathbb{Z}_p$ and the cantor set $\mathcal{C}^p$.

Metric topology of $\mathbb{Q}_p$: Euclidean Models of $\mathbb{Z}_p$

Sets of $\mathbb{R}^n$ that are homeomorphic to $\mathbb{Z}_p$ are called Euclidean models.

one-dimensional

The following map

$$\sum_{n=0}^{\infty} a_n 2^n \mapsto \sum_{n=0}^{\infty} \frac{2a_n}{3^{n+1}}$$

gives a homeomorphism between $\mathbb{Z}_2$ and the cantor set $\mathcal{C}$.

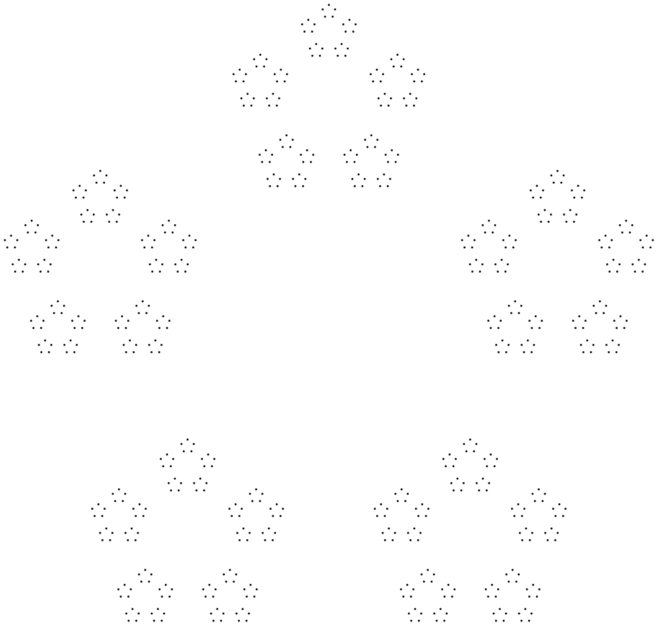
You can construct Cantor-like sets $\mathcal{C}^p$, where numbers can be written in base $2p-1$; starting with the unit interval, and continuing recursively, divide into $2p-1$ pieces and delete the second piece. Taking the intersection of the resulting pieces gives you $\mathcal{C}^p$.The following map

$$\sum_{n=0}^{\infty} a_n p^n \mapsto \sum_{n=0}^{\infty} \frac{2a_n}{(2p-1)^{n+1}}$$

gives a homeomorphism between $\mathbb{Z}_p$ and the cantor set $\mathcal{C}^p$.

two-dimensional

Will skip the technical details, not that hard! Here's one model of $\mathbb{Z}_5$.



Functions in $\mathbb{Q}_p$: series & power series

Functions in $\mathbb{Q}_p$: series & power series

Series are simpler to study with respect to $|\cdot|_p$

Series are simpler to study with respect to $|\cdot|_p$

convergence of series

Functions in $\mathbb{Q}_p$: series & power series

Series are simpler to study with respect to $|\cdot|_p$

convergence of series

A p-adic series

$$\sum_{n=1}^{\infty} c_n, \quad c_n \in \mathbb{Q}_p$$

converges if

Functions in $\mathbb{Q}_p$: series & power series

Series are simpler to study with respect to $|\cdot|_p$

convergence of series

A p-adic series

$$\sum_{n=1}^{\infty} c_n, \quad c_n \in \mathbb{Q}_p$$

converges if and only if $|c_n|_p \to 0$.

Functions in $\mathbb{Q}_p$: series & power series

Series are simpler to study with respect to $|\cdot|_p$

convergence of series

A p-adic series

$$\sum_{n=1}^{\infty} c_n, \quad c_n \in \mathbb{Q}_p$$

converges if and only if $|c_n|_p \to 0$.

radius of convergence

Functions in $\mathbb{Q}_p$: series & power series

Series are simpler to study with respect to $|\cdot|_p$

convergence of series

A p-adic series

$$\sum_{n=1}^{\infty} c_n, \quad c_n \in \mathbb{Q}_p$$

converges if and only if $|c_n|_p \to 0$.

radius of convergence

As usual, given a power series

$$f(x) = \sum_{n=1}^{\infty} a_n x^n$$

we can determine its radius of convergence, which is given by

$$R = \frac{1}{\limsup_{n\to\infty} |a_n|_p^{1/n}}$$

Functions in $\mathbb{Q}_p$: series & power series

Series are simpler to study with respect to $|\cdot|_p$

convergence of series

A p-adic series

$$\sum_{n=1}^{\infty} c_n, \quad c_n \in \mathbb{Q}_p$$

converges if and only if $|c_n|_p \to 0$.

radius of convergence

As usual, given a power series

$$f(x) = \sum_{n=1}^{\infty} a_n x^n$$

we can determine its radius of convergence, which is given by

$$R = \frac{1}{\limsup_{n\to\infty} |a_n|_p^{1/n}}$$

Functions in $\mathbb{Q}_p$: problems with familiar functions

Exponential

Functions in $\mathbb{Q}_p$: problems with familiar functions

Exponential

Consider

$$\operatorname{Exp}(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

It's radius of convergence is

Functions in $\mathbb{Q}_p$: problems with familiar functions

Exponential

Consider

$$\mathrm{Exp}(x) \coloneqq \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

It's radius of convergence is **not** ∞

Exponential

Consider

$$\operatorname{Exp}(x) \coloneqq \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

It's radius of convergence is **not** ∞, it is $p^{-1/(p-1)}$.

Functions in $\mathbb{Q}_p$: problems with familiar functions

Exponential

Consider

$$\mathrm{Exp}(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

It's radius of convergence is **not** ∞, it is $p^{-1/(p-1)}$.

There's a very important candidate of the exponential function called the Artin-Hasse exponential, which has a slightly larger radius of convergence.

Functions in $\mathbb{Q}_p$: problems with familiar functions

Exponential

Consider

$$\operatorname{Exp}(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

It's radius of convergence is **not** ∞, it is $p^{-1/(p-1)}$.

There's a very important candidate of the exponential function called the Artin-Hasse exponential, which has a slightly larger radius of convergence.

Logarithms

Functions in $\mathbb{Q}_p$: problems with familiar functions

Exponential

Consider

$$\mathrm{Exp}(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

It's radius of convergence is **not** ∞, it is $p^{-1/(p-1)}$.

There's a very important candidate of the exponential function called the Artin-Hasse exponential, which has a slightly larger radius of convergence.

Logarithms

The series

$$-\log_p(1-x) := \sum_{n=1}^{\infty} \frac{x^n}{n}$$

converges in the region $|x|_p < 1$

Functions in $\mathbb{Q}_p$: continuous functions $C(\mathbb{Z}_p, \mathbb{Q}_p)$

$C([0,1], \mathbb{R})$, the set of all continuous functions $f : [0,1] \to \mathbb{R}$ is a first example of a function space in real analysis

Functions in $\mathbb{Q}_p$: continuous functions $C(\mathbb{Z}_p, \mathbb{Q}_p)$

$C([0,1],\mathbb{R})$, the set of all continuous functions $f : [0,1] \to \mathbb{R}$ is a first example of a function space in real analysis, it's p-adic analogue is $C(\mathbb{Z}_p, \mathbb{Q}_p)$, the set of all continuous functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$.

Functions in $\mathbb{Q}_p$: continuous functions $C(\mathbb{Z}_p, \mathbb{Q}_p)$

$C([0,1], \mathbb{R})$, the set of all continuous functions $f : [0,1] \to \mathbb{R}$ is a first example of a function space in real analysis, it's p-adic analogue is $C(\mathbb{Z}_p, \mathbb{Q}_p)$, the set of all continuous functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$. They're in fact Banach spaces with respect to the sup-norm.

$C([0,1], \mathbb{R})$, the set of all continuous functions $f : [0,1] \longrightarrow \mathbb{R}$ is a first example of a function space in real analysis, it's p-adic analogue is $C(\mathbb{Z}_p, \mathbb{Q}_p)$, the set of all continuous functions $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$. They're in fact Banach spaces with respect to the sup-norm.

In both $C([0,1], \mathbb{R})$ and $C(\mathbb{Z}_p, \mathbb{Q}_p)$, the polynomial functions are a dense subset

$C([0,1], \mathbb{R})$, the set of all continuous functions $f : [0,1] \to \mathbb{R}$ is a first example of a function space in real analysis, it's p-adic analogue is $C(\mathbb{Z}_p, \mathbb{Q}_p)$, the set of all continuous functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$. They're in fact Banach spaces with respect to the sup-norm.

In both $C([0,1], \mathbb{R})$ and $C(\mathbb{Z}_p, \mathbb{Q}_p)$, the polynomial functions are a dense subset, the former is by Weierstrass (1885) and the latter was first proven by Dieudonne (1944).

Functions in $\mathbb{Q}_p$: continuous functions $C(\mathbb{Z}_p, \mathbb{Q}_p)$

$C([0,1], \mathbb{R})$, the set of all continuous functions $f : [0,1] \to \mathbb{R}$ is a first example of a function space in real analysis, it's p-adic analogue is $C(\mathbb{Z}_p, \mathbb{Q}_p)$, the set of all continuous functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$. They're in fact Banach spaces with respect to the sup-norm.

In both $C([0,1], \mathbb{R})$ and $C(\mathbb{Z}_p, \mathbb{Q}_p)$, the polynomial functions are a dense subset, the former is by Weierstrass (1885) and the latter was first proven by Dieudonne (1944).

While there exists no nice description of $C([0,1], \mathbb{R})$, there does exist one for $C(\mathbb{Z}_p, \mathbb{Q}_p)$!

Theorem (Mahler, 1961)

Functions in $\mathbb{Q}_p$: Mahler's Theorem

Theorem (Mahler, 1961)

Suppose $f : \mathbb{Z}_p \to \mathbb{Q}_p$ can be written as is continuous.

Theorem (Mahler, 1961)

Suppose $f : \mathbb{Z}_p \to \mathbb{Q}_p$ can be written as is continuous. Let

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k)$$

Theorem (Mahler, 1961)

Suppose $f : \mathbb{Z}_p \to \mathbb{Q}_p$ can be written as is continuous. Let

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k)$$

Then $a_n(f) \to 0$

Theorem (Mahler, 1961)

Suppose $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ can be written as is continuous. Let

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k)$$

Then $a_n(f) \longrightarrow 0$, and so the series

$$\sum_{k=0}^{\infty} a_n(f) \binom{x}{n}$$

converges uniformly in $\mathbb{Z}_p$.

Theorem (Mahler, 1961)

Suppose $f : \mathbb{Z}_p \to \mathbb{Q}_p$ can be written as is continuous. Let

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k)$$

Then $a_n(f) \to 0$, and so the series

$$\sum_{k=0}^{\infty} a_n(f) \binom{x}{n}$$

converges uniformly in $\mathbb{Z}_p$. Moreover,

$$f(x) = \sum_{k=0}^{\infty} a_n(f) \binom{x}{n}$$

Hensel's Lemma: statement(s)

Hensel's Lemma: statement(s)

Hensel's Lemma (Lifting roots mod p)

Hensel's Lemma (Lifting roots mod p)

Let $f(x) \in \mathbb{Z}_p[x]$, and suppose there exists a $a \in \mathbb{Z}_p$ such that

$$f(a) \equiv 0 \bmod p \quad \text{and} \quad f'(a) \not\equiv 0 \bmod p$$

Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv a \bmod p$ and $f(\alpha) = 0$.

Hensel's Lemma (Lifting roots mod p)

Let $f(x) \in \mathbb{Z}_p[x]$, and suppose there exists a $a \in \mathbb{Z}_p$ such that

$$f(a) \equiv 0 \bmod p \quad \text{and} \quad f'(a) \not\equiv 0 \bmod p$$

Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv a \bmod p$ and $f(\alpha) = 0$.

Hensel's Lemma (p-adic Newton-Raphson)

Hensel's Lemma: statement(s)

Hensel's Lemma (Lifting roots mod p)

Let $f(x) \in \mathbb{Z}_p[x]$, and suppose there exists a $a \in \mathbb{Z}_p$ such that

$$f(a) \equiv 0 \bmod p \quad \text{and} \quad f'(a) \not\equiv 0 \bmod p$$

Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv a \bmod p$ and $f(\alpha) = 0$.

Hensel's Lemma (p-adic Newton-Raphson)

Let $f(x) \in \mathbb{Z}_p[x]$, and suppose there exists a $a_1 \in \mathbb{Z}_p$ such that $|f(a_1)|_p < 1$ and $|f'(a_1)|_p = 1$. Then, for each $n \geq 1$

$$a_{n+1} \coloneqq a_n - \frac{f(a_n)}{f'(a_n)}$$

defines a convergent sequence whose limit $\alpha \in \mathbb{Z}_p$ is the unique p-adic integer such that $|\alpha - a_1| < 1$ and $f(\alpha) = 0$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv a \bmod p$ and $f(\alpha) = 0$.

Hensel's Lemma: polynomial version

Hensel’s Lemma: polynomial version

Polynomial Form of Hensel’s Lemma (Lifting factors mod p)

Hensel's Lemma: polynomial version

Polynomial Form of Hensel's Lemma (Lifting factors mod p)

Let $f(x) \in \mathbb{Z}_p[x]$, and suppose there exist $G(x), H(x) \in \mathbb{F}_p[x]$ such that

$$f(x) \equiv G(x)H(x) \bmod p$$

with $(G, H) = 1$, and $G(x)$ monic. Then there exist polynomials $g(x), h(x) \in \mathbb{Z}_p[x]$ such that $g(x) \equiv G(x) \bmod p$, $h(x) \equiv H(x) \bmod p$ with $g(x)$ monic and

$$f(x) = g(x)h(x)$$

Hensel's Lemma: applications

roots of unity

roots of unity

For any prime p and any positive integer m not divisible by p, there exists a primitive m^{th} root of unity in $\mathbb{Q}_p$ if and only if m divides $p-1$.

Hensel's Lemma: applications

roots of unity

For any prime p and any positive integer m not divisible by p, there exists a primitive m^{th} root of unity in $\mathbb{Q}_p$ if and only if m divides $p-1$.

squares

Hensel's Lemma: applications

roots of unity

For any prime p and any positive integer m not divisible by p, there exists a primitive m^{th} root of unity in $\mathbb{Q}_p$ if and only if m divides $p-1$.

squares

For $p \neq 2$, $x = p^n u \in \mathbb{Q}_p^\times$ is a square if and only if n is even and u is a square mod p.

roots of unity

For any prime p and any positive integer m not divisible by p, there exists a primitive m^{th} root of unity in $\mathbb{Q}_p$ if and only if m divides $p-1$.

squares

For $p \neq 2$, $x = p^n u \in \mathbb{Q}_p^\times$ is a square if and only if n is even and u is a square mod p. We have $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

For $p = 2$, $x = 2^n u \in \mathbb{Q}_2^\times$ is a square if and only if n is even and $u \equiv 1 \bmod 8$.

Hensel's Lemma: applications

roots of unity

For any prime p and any positive integer m not divisible by p, there exists a primitive m^{th} root of unity in $\mathbb{Q}_p$ if and only if m divides $p-1$.

squares

For $p \neq 2$, $x = p^n u \in \mathbb{Q}_p^\times$ is a square if and only if n is even and u is a square mod p. We have $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

For $p = 2$, $x = 2^n u \in \mathbb{Q}_2^\times$ is a square if and only if n is even and $u \equiv 1 \bmod 8$. We have $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

roots of unity

For any prime p and any positive integer m not divisible by p, there exists a primitive m^{th} root of unity in $\mathbb{Q}_p$ if and only if m divides $p-1$.

squares

For $p \neq 2$, $x = p^n u \in \mathbb{Q}_p^\times$ is a square if and only if n is even and u is a square mod p. We have $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

For $p = 2$, $x = 2^n u \in \mathbb{Q}_2^\times$ is a square if and only if n is even and $u \equiv 1 \bmod 8$. We have $\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Recall $\mathbb{R}^\times / \mathbb{R}^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$.

Local and Global: towards the principal

Local and Global: towards the principal

For this section, $\mathbb{Q}_\infty \coloneqq \mathbb{R}$.

For this section, $\mathbb{Q}_\infty \coloneqq \mathbb{R}$.

first examples

Let's think about rational roots of polynomials. If there's a root in $\mathbb{Q}$, then there are roots in $\mathbb{Q}_p$ for all $p \leq \infty$, contrapositive can give us non-existence.

For this section, $\mathbb{Q}_\infty \coloneqq \mathbb{R}$.

first examples

Let's think about rational roots of polynomials. If there's a root in $\mathbb{Q}$, then there are roots in $\mathbb{Q}_p$ for all $p \leq \infty$, contrapositive can give us non-existence. For example,

- $x^2 + 1 = 0$ has no roots in $\mathbb{Q}_\infty$, hence has none in $\mathbb{Q}$.

For this section, $\mathbb{Q}_\infty \coloneqq \mathbb{R}$.

first examples

Let's think about rational roots of polynomials. If there's a root in $\mathbb{Q}$, then there are roots in $\mathbb{Q}_p$ for all $p \leq \infty$, contrapositive can give us non-existence. For example,

- $x^2 + 1 = 0$ has no roots in $\mathbb{Q}_\infty$, hence has none in $\mathbb{Q}$.
- $x^2 - 2 = 0$ has no roots in $\mathbb{Q}_2$, hence has none in $\mathbb{Q}$.

For this section, $\mathbb{Q}_\infty \coloneqq \mathbb{R}$.

first examples

Let's think about rational roots of polynomials. If there's a root in $\mathbb{Q}$, then there are roots in $\mathbb{Q}_p$ for all $p \leq \infty$, contrapositive can give us non-existence. For example,

- $x^2 + 1 = 0$ has no roots in $\mathbb{Q}_\infty$, hence has none in $\mathbb{Q}$.
- $x^2 - 2 = 0$ has no roots in $\mathbb{Q}_2$, hence has none in $\mathbb{Q}$.
- The only solution of $x^2 - 37y^2 = 0$ in $\mathbb{Q}_5$ is $x = y = 0$, so that is also the only solution in $\mathbb{Q}$.

For this section, $\mathbb{Q}_\infty \coloneqq \mathbb{R}$.

first examples

Let's think about rational roots of polynomials. If there's a root in $\mathbb{Q}$, then there are roots in $\mathbb{Q}_p$ for all $p \leq \infty$, contrapositive can give us non-existence. For example,

- $x^2 + 1 = 0$ has no roots in $\mathbb{Q}_\infty$, hence has none in $\mathbb{Q}$.
- $x^2 - 2 = 0$ has no roots in $\mathbb{Q}_2$, hence has none in $\mathbb{Q}$.
- The only solution of $x^2 - 37y^2 = 0$ in $\mathbb{Q}_5$ is $x = y = 0$, so that is also the only solution in $\mathbb{Q}$.

These are examples of "global to local".

For this section, $\mathbb{Q}_\infty \coloneqq \mathbb{R}$.

first examples

Let's think about rational roots of polynomials. If there's a root in $\mathbb{Q}$, then there are roots in $\mathbb{Q}_p$ for all $p \leq \infty$, contrapositive can give us non-existence. For example,

- $x^2 + 1 = 0$ has no roots in $\mathbb{Q}_\infty$, hence has none in $\mathbb{Q}$.
- $x^2 - 2 = 0$ has no roots in $\mathbb{Q}_2$, hence has none in $\mathbb{Q}$.
- The only solution of $x^2 - 37y^2 = 0$ in $\mathbb{Q}_5$ is $x = y = 0$, so that is also the only solution in $\mathbb{Q}$.

These are examples of "global to local".

Kurt Hensel (the one who "discovered" the p-adics) hoped that "local" roots could be patched to give "global" roots.

For this section, $\mathbb{Q}_\infty := \mathbb{R}$.

first examples

Let's think about rational roots of polynomials. If there's a root in $\mathbb{Q}$, then there are roots in $\mathbb{Q}_p$ for all $p \leq \infty$, contrapositive can give us non-existence. For example,

- $x^2 + 1 = 0$ has no roots in $\mathbb{Q}_\infty$, hence has none in $\mathbb{Q}$.
- $x^2 - 2 = 0$ has no roots in $\mathbb{Q}_2$, hence has none in $\mathbb{Q}$.
- The only solution of $x^2 - 37y^2 = 0$ in $\mathbb{Q}_5$ is $x = y = 0$, so that is also the only solution in $\mathbb{Q}$.

These are examples of "global to local".

Kurt Hensel (the one who "discovered" the p-adics) hoped that "local" roots could be patched to give "global" roots.

an example of "local to global"

A number $x \in \mathbb{Q}$ is a square if and only if it is a square in every $\mathbb{Q}_p$, $p \leq \infty$.

Local and Global: the principal, in practice

Local and Global: the principal, in practice

Local-Global Principal

Local and Global: the principal, in practice

Local-Global Principal

The existence or non-existence of solutions in $\mathbb{Q}$ (global solutions) of a diophantine equation can be detected by studying, for each $p \leq \infty$, the solutions of the equation in $\mathbb{Q}_p$ (local solutions).

Local and Global: the principal, in practice

Local-Global Principal

The existence or non-existence of solutions in $\mathbb{Q}$ (global solutions) of a diophantine equation can be detected by studying, for each $p \leq \infty$, the solutions of the equation in $\mathbb{Q}_p$ (local solutions).

This is also called the Hasse principal, after Helmut Hasse, a student of Hensel, who proved the first theorem that justified this principal.

Local-Global Principal

The existence or non-existence of solutions in $\mathbb{Q}$ (global solutions) of a diophantine equation can be detected by studying, for each $p \leq \infty$, the solutions of the equation in $\mathbb{Q}_p$ (local solutions).

This is also called the Hasse principal, after Helmut Hasse, a student of Hensel, who proved the first theorem that justified this principal.

Theorem (Hasse-Minkowski)

Let

$$F(x_1, x_2, \ldots, x_n) = \sum_{i,j} c_{ij} x_i x_j \in \mathbb{Q}[x_1, x_2, \ldots, x_n]$$

be a quadratic form (that is, a homogeneous polynomial of degree 2 in n variables). The equation

$$F(x_1, x_2, \ldots, x_n) = 0$$

has non-trivial solutions in Q if and only if it has non-trivial solutions in $\mathbb{Q}_p$ for each $p \leq \infty$.

Local and Global: hopes and failure

Local and Global: hopes and failure

Unfortunately, this principal fails to hold completely beyond degree 2.

Local and Global: hopes and failure

Unfortunately, this principal fails to hold completely beyond degree 2.

examples of failure of Local-Global

The following equations have a solution in $\mathbb{Q}_p$ for all $p \leq \infty$, but have no roots in $\mathbb{Q}$

Unfortunately, this principal fails to hold completely beyond degree 2.

examples of failure of Local-Global

The following equations have a solution in $\mathbb{Q}_p$ for all $p \leq \infty$, but have no roots in $\mathbb{Q}$

- $(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$

Unfortunately, this principal fails to hold completely beyond degree 2.

examples of failure of Local-Global

The following equations have a solution in $\mathbb{Q}_p$ for all $p \leq \infty$, but have no roots in $\mathbb{Q}$

- $(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$
- $x^4 - 17 = 2y^2$

Unfortunately, this principal fails to hold completely beyond degree 2.

examples of failure of Local-Global

The following equations have a solution in $\mathbb{Q}_p$ for all $p \leq \infty$, but have no roots in $\mathbb{Q}$

- $(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$
- $x^4 - 17 = 2y^2$

Algebro-geometrically, local information is not enough to determine $\mathbb{Q}$-points of genus 1 and higher curves.

Unfortunately, this principal fails to hold completely beyond degree 2.

examples of failure of Local-Global

The following equations have a solution in $\mathbb{Q}_p$ for all $p \leq \infty$, but have no roots in $\mathbb{Q}$

- $(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$
- $x^4 - 17 = 2y^2$

Algebro-geometrically, local information is not enough to determine $\mathbb{Q}$-points of genus 1 and higher curves.

But, you can still hope for local information telling you something about the global picture.

Beyond $\mathbb{Q}_p$: a quick download

some quick facts

some quick facts

- Unexpectedly, $\mathbb{Q}_p$ is not algebraically closed.

some quick facts

- Unexpectedly, $\mathbb{Q}_p$ is not algebraically closed.
- But unlike $\mathbb{R}$, it's not a finite extension away from being so.

Beyond $\mathbb{Q}_p$: a quick download

some quick facts

- Unexpectedly, $\mathbb{Q}_p$ is not algebraically closed.
- But unlike $\mathbb{R}$, it's not a finite extension away from being so.
- So there's a whole host of finite extensions of $\mathbb{Q}_p$ that can be studied, they're called local number fields.

Beyond $\mathbb{Q}_p$: a quick download

some quick facts

- Unexpectedly, $\mathbb{Q}_p$ is not algebraically closed.
- But unlike $\mathbb{R}$, it's not a finite extension away from being so.
- So there's a whole host of finite extensions of $\mathbb{Q}_p$ that can be studied, they're called local number fields.
- This study could very well be called p-adic algebraic number theory.

some quick facts

- Unexpectedly, $\mathbb{Q}_p$ is not algebraically closed.
- But unlike $\mathbb{R}$, it's not a finite extension away from being so.
- So there's a whole host of finite extensions of $\mathbb{Q}_p$ that can be studied, they're called local number fields.
- This study could very well be called p-adic algebraic number theory.
- Except local number fields are complete normed spaces with respect to a unique non-Archimedean extension of $|\cdot|_p$ on $\mathbb{Q}_p$.

some quick facts

- Unexpectedly, $\mathbb{Q}_p$ is not algebraically closed.
- But unlike $\mathbb{R}$, it's not a finite extension away from being so.
- So there's a whole host of finite extensions of $\mathbb{Q}_p$ that can be studied, they're called local number fields.
- This study could very well be called p-adic algebraic number theory.
- Except local number fields are complete normed spaces with respect to a unique non-Archimedean extension of $|\cdot|_p$ on $\mathbb{Q}_p$.
- The unit closed balls are the analogues of rings of integers, and they're local rings, similar to $\mathbb{Z}_p$.

Beyond $\mathbb{Q}_p$: a quick download

some quick facts

- Unexpectedly, $\mathbb{Q}_p$ is not algebraically closed.
- But unlike $\mathbb{R}$, it's not a finite extension away from being so.
- So there's a whole host of finite extensions of $\mathbb{Q}_p$ that can be studied, they're called local number fields.
- This study could very well be called p-adic algebraic number theory.
- Except local number fields are complete normed spaces with respect to a unique non-Archimedean extension of $|\cdot|_p$ on $\mathbb{Q}_p$.
- The unit closed balls are the analogues of rings of integers, and they're local rings, similar to $\mathbb{Z}_p$.
- You can make sense of ramification index and residue degree, and so talk about ramified and unramified extensions.

Beyond $\mathbb{Q}_p$: a quick download

some quick facts

- Unexpectedly, $\mathbb{Q}_p$ is not algebraically closed.
- But unlike $\mathbb{R}$, it's not a finite extension away from being so.
- So there's a whole host of finite extensions of $\mathbb{Q}_p$ that can be studied, they're called local number fields.
- This study could very well be called p-adic algebraic number theory.
- Except local number fields are complete normed spaces with respect to a unique non-Archimedean extension of $|\cdot|_p$ on $\mathbb{Q}_p$.
- The unit closed balls are the analogues of rings of integers, and they're local rings, similar to $\mathbb{Z}_p$.
- You can make sense of ramification index and residue degree, and so talk about ramified and unramified extensions.
- What do they look like? Set theoretically, with each extension, you allow for fractional powers in the Laurent series expansion. The closure allows any fractional power.

Beyond $\mathbb{Q}_p$: a quick download

some quick facts

- Unexpectedly, $\mathbb{Q}_p$ is not algebraically closed.
- But unlike $\mathbb{R}$, it's not a finite extension away from being so.
- So there's a whole host of finite extensions of $\mathbb{Q}_p$ that can be studied, they're called local number fields.
- This study could very well be called p-adic algebraic number theory.
- Except local number fields are complete normed spaces with respect to a unique non-Archimedean extension of $|\cdot|_p$ on $\mathbb{Q}_p$.
- The unit closed balls are the analogues of rings of integers, and they're local rings, similar to $\mathbb{Z}_p$.
- You can make sense of ramification index and residue degree, and so talk about ramified and unramified extensions.
- What do they look like? Set theoretically, with each extension, you allow for fractional powers in the Laurent series expansion. The closure allows any fractional power.

Beyond $\mathbb{Q}_p$: irreducibility criterions and extensions

Gauss's Lemma in $\mathbb{Q}_p$

Gauss's Lemma in $\mathbb{Q}_p$

Suppose that $f(x) \in \mathbb{Z}_p[x]$ factors in $\mathbb{Q}_p[x]$, so that $f(x) = g(x)h(x)$, with $g(x), h(x) \in \mathbb{Q}_p[x]$ and non-constant.

Gauss's Lemma in $\mathbb{Q}_p$

Suppose that $f(x) \in \mathbb{Z}_p[x]$ factors in $\mathbb{Q}_p[x]$, so that $f(x) = g(x)h(x)$, with $g(x), h(x) \in \mathbb{Q}_p[x]$ and non-constant. Then there exist non-constant polynomials $g_0(x), h_0(x) \in \mathbb{Z}_p[x]$ such that $f(x) = g_0(x)h_0(x)$.

Gauss's Lemma in $\mathbb{Q}_p$

Suppose that $f(x) \in \mathbb{Z}_p[x]$ factors in $\mathbb{Q}_p[x]$, so that $f(x) = g(x)h(x)$, with $g(x), h(x) \in \mathbb{Q}_p[x]$ and non-constant. Then there exist non-constant polynomials $g_0(x), h_0(x) \in \mathbb{Z}_p[x]$ such that $f(x) = g_0(x)h_0(x)$.

Corollary I

Gauss's Lemma in $\mathbb{Q}_p$

Suppose that $f(x) \in \mathbb{Z}_p[x]$ factors in $\mathbb{Q}_p[x]$, so that $f(x) = g(x)h(x)$, with $g(x), h(x) \in \mathbb{Q}_p[x]$ and non-constant. Then there exist non-constant polynomials $g_0(x), h_0(x) \in \mathbb{Z}_p[x]$ such that $f(x) = g_0(x)h_0(x)$.

Corollary I

Let $f(x) \in \mathbb{Z}_p[x]$ be a monic polynomial whose reduction mod p is irreducible in $\mathbb{F}_p[x]$. Then $f(x)$ is irreducible over $\mathbb{Q}_p$.

Beyond $\mathbb{Q}_p$: irreducibility criterions and extensions

Gauss's Lemma in $\mathbb{Q}_p$

Suppose that $f(x) \in \mathbb{Z}_p[x]$ factors in $\mathbb{Q}_p[x]$, so that $f(x) = g(x)h(x)$, with $g(x), h(x) \in \mathbb{Q}_p[x]$ and non-constant. Then there exist non-constant polynomials $g_0(x), h_0(x) \in \mathbb{Z}_p[x]$ such that $f(x) = g_0(x)h_0(x)$.

Corollary I

Let $f(x) \in \mathbb{Z}_p[x]$ be a monic polynomial whose reduction mod p is irreducible in $\mathbb{F}_p[x]$. Then $f(x)$ is irreducible over $\mathbb{Q}_p$.

Corollary II

For each integer $n \geq 1$ there is an extension of $\mathbb{Q}_p$ which has degree exactly n and which "comes from" the unique extension of degree n of the finite field $\mathbb{F}_p$.

Beyond $\mathbb{Q}_p$: irreducibility criterions and extensions

Gauss's Lemma in $\mathbb{Q}_p$

Suppose that $f(x) \in \mathbb{Z}_p[x]$ factors in $\mathbb{Q}_p[x]$, so that $f(x) = g(x)h(x)$, with $g(x), h(x) \in \mathbb{Q}_p[x]$ and non-constant. Then there exist non-constant polynomials $g_0(x), h_0(x) \in \mathbb{Z}_p[x]$ such that $f(x) = g_0(x)h_0(x)$.

Corollary I

Let $f(x) \in \mathbb{Z}_p[x]$ be a monic polynomial whose reduction mod p is irreducible in $\mathbb{F}_p[x]$. Then $f(x)$ is irreducible over $\mathbb{Q}_p$.

Corollary II

For each integer $n \geq 1$ there is an extension of $\mathbb{Q}_p$ which has degree exactly n and which "comes from" the unique extension of degree n of the finite field $\mathbb{F}_p$. In particular, the algebraic closure $\mathbb{Q}_p$ is an infinite extension of $\mathbb{Q}_p$.

Beyond $\mathbb{Q}_p$: extension of $|\cdot|_p$

a finite extension of $\mathbb{Q}_p$ is a complete ultrametric space

a finite extension of $\mathbb{Q}_p$ is a complete ultrametric space

Let $K/\mathbb{Q}_p$ be a finite extension of degree n. The function $|\cdot|_p^K : K \longrightarrow \mathbb{R}_+$ defined by

$$|x|_p^K = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

is a unique non-Archimedean norm on K which extends the $|\cdot|_p$ on $\mathbb{Q}_p$.

Beyond $\mathbb{Q}_p$: extension of $|\cdot|_p$

a finite extension of $\mathbb{Q}_p$ is a complete ultrametric space

Let $K/\mathbb{Q}_p$ be a finite extension of degree n. The function $|\cdot|_p^K : K \to \mathbb{R}_+$ defined by

$$|x|_p^K = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

is a unique non-Archimedean norm on K which extends the $|\cdot|_p$ on $\mathbb{Q}_p$. K is a complete normed space with respect to $|\cdot|_p^K$.

Beyond $\mathbb{Q}_p$: extension of $|\cdot|_p$

a finite extension of $\mathbb{Q}_p$ is a complete ultrametric space

Let $K/\mathbb{Q}_p$ be a finite extension of degree n. The function $|\cdot|_p^K : K \to \mathbb{R}_+$ defined by

$$|x|_p^K = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

is a unique non-Archimedean norm on K which extends the $|\cdot|_p$ on $\mathbb{Q}_p$. K is a complete normed space with respect to $|\cdot|_p^K$.

$\overline{\mathbb{Q}_p}$ is a ultrametric space

Beyond $\mathbb{Q}_p$: extension of $|\cdot|_p$

a finite extension of $\mathbb{Q}_p$ is a complete ultrametric space

Let $K/\mathbb{Q}_p$ be a finite extension of degree n. The function $|\cdot|_p^K : K \to \mathbb{R}_+$ defined by

$$|x|_p^K = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

is a unique non-Archimedean norm on K which extends the $|\cdot|_p$ on $\mathbb{Q}_p$. K is a complete normed space with respect to $|\cdot|_p^K$.

$\overline{\mathbb{Q}_p}$ is a ultrametric space

Given any $\alpha \in \overline{\mathbb{Q}_p}$, the extension $\mathbb{Q}_p(\alpha)$ is finite. So define $|\alpha|_p^{\overline{\mathbb{Q}_p}} := |\alpha|_p^{\mathbb{Q}_p(\alpha)}$.

a finite extension of $\mathbb{Q}_p$ is a complete ultrametric space

Let $K/\mathbb{Q}_p$ be a finite extension of degree n. The function $|\cdot|_p^K : K \to \mathbb{R}_+$ defined by

$$|x|_p^K = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

is a unique non-Archimedean norm on K which extends the $|\cdot|_p$ on $\mathbb{Q}_p$. K is a complete normed space with respect to $|\cdot|_p^K$.

$\overline{\mathbb{Q}_p}$ is a ultrametric space

Given any $\alpha \in \overline{\mathbb{Q}}_p$, the extension $\mathbb{Q}_p(\alpha)$ is finite. So define $|\alpha|_p^{\overline{\mathbb{Q}}_p} := |\alpha|_p^{\mathbb{Q}_p(\alpha)}$.

Problem: $\overline{\mathbb{Q}}_p$ isn't complete! (Contrast with $\overline{\mathbb{R}} = \mathbb{C}$.)

Beyond $\mathbb{Q}_p$: finite extensions

Beyond $\mathbb{Q}_p$: finite extensions

Local Number Fields

Local Number Fields

Let $K/\mathbb{Q}_p$ be a finite extension of degree n and let $|\cdot| := |\cdot|_p^K$

Local Number Fields

Let $K/\mathbb{Q}_p$ be a finite extension of degree n and let $|\cdot| \coloneqq |\cdot|_p^K$, and define

$$\mathcal{O}_K \coloneqq \{x \in K \mid |x| \leq 1\}.$$

Local Number Fields

Let $K/\mathbb{Q}_p$ be a finite extension of degree n and let $|\cdot| := |\cdot|_p^K$, and define

$$\mathcal{O}_K := \{x \in K \mid |x| \leq 1\}.$$

Then $\mathcal{O}_K$ is a local ring, with

$$\mathfrak{m}_K := \{x \in K \mid |x| < 1\}$$

as its unique maximal ideal.

Local Number Fields

Let $K/\mathbb{Q}_p$ be a finite extension of degree n and let $|\cdot| := |\cdot|_p^K$, and define

$$\mathcal{O}_K := \{x \in K \mid |x| \leq 1\}.$$

Then $\mathcal{O}_K$ is a local ring, with

$$\mathfrak{m}_K := \{x \in K \mid |x| < 1\}$$

as its unique maximal ideal. There exists an element $\pi \in \mathcal{O}_K$ (called the uniformizer) of maximal norm less than 1 such that $\mathfrak{m}_K = \pi\mathcal{O}_K$.

Local Number Fields

Let $K/\mathbb{Q}_p$ be a finite extension of degree n and let $|\cdot| \coloneqq |\cdot|_p^K$, and define

$$\mathcal{O}_K \coloneqq \{x \in K \mid |x| \leq 1\}.$$

Then $\mathcal{O}_K$ is a local ring, with

$$\mathfrak{m}_K \coloneqq \{x \in K \mid |x| < 1\}$$

as its unique maximal ideal. There exists an element $\pi \in \mathcal{O}_K$ (called the uniformizer) of maximal norm less than 1 such that $\mathfrak{m}_K = \pi\mathcal{O}_K$.

The residue field $\kappa = \mathcal{O}_K/\mathfrak{m}_K$ is finite and therefore a finite extension of $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$.

Local Number Fields

Let $K/\mathbb{Q}_p$ be a finite extension of degree n and let $|\cdot| := |\cdot|_p^K$, and define

$$\mathcal{O}_K := \{x \in K \mid |x| \leq 1\}.$$

Then $\mathcal{O}_K$ is a local ring, with

$$\mathfrak{m}_K := \{x \in K \mid |x| < 1\}$$

as its unique maximal ideal. There exists an element $\pi \in \mathcal{O}_K$ (called the uniformizer) of maximal norm less than 1 such that $\mathfrak{m}_K = \pi\mathcal{O}_K$.

The residue field $\kappa = \mathcal{O}_K/\mathfrak{m}_K$ is finite and therefore a finite extension of $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$.The **residue degree** is defined as $f := [\kappa : \mathbb{F}_p]$.

Local Number Fields

Let $K/\mathbb{Q}_p$ be a finite extension of degree n and let $|\cdot| := |\cdot|_p^K$, and define

$$\mathcal{O}_K := \{x \in K \mid |x| \leq 1\}.$$

Then $\mathcal{O}_K$ is a local ring, with

$$\mathfrak{m}_K := \{x \in K \mid |x| < 1\}$$

as its unique maximal ideal. There exists an element $\pi \in \mathcal{O}_K$ (called the uniformizer) of maximal norm less than 1 such that $\mathfrak{m}_K = \pi\mathcal{O}_K$.

The residue field $\kappa = \mathcal{O}_K/\mathfrak{m}_K$ is finite and therefore a finite extension of $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$.The **residue degree** is defined as $f := [\kappa : \mathbb{F}_p]$.

We have $p \in \pi\mathcal{O}_K$, there exists some $e \geq 1$ such that $|p| = |\pi|^e$. e is called the **ramification index**.

Local Number Fields

Let $K/\mathbb{Q}_p$ be a finite extension of degree n and let $|\cdot| := |\cdot|_p^K$, and define

$$\mathcal{O}_K := \{x \in K \mid |x| \leq 1\}.$$

Then $\mathcal{O}_K$ is a local ring, with

$$\mathfrak{m}_K := \{x \in K \mid |x| < 1\}$$

as its unique maximal ideal. There exists an element $\pi \in \mathcal{O}_K$ (called the uniformizer) of maximal norm less than 1 such that $\mathfrak{m}_K = \pi\mathcal{O}_K$.

The residue field $\kappa = \mathcal{O}_K/\mathfrak{m}_K$ is finite and therefore a finite extension of $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$.The **residue degree** is defined as $f := [\kappa : \mathbb{F}_p]$.

We have $p \in \pi\mathcal{O}_K$, there exists some $e \geq 1$ such that $|p| = |\pi|^e$. e is called the **ramification index**.

As you will hope from my experiences with classic algebraic number theory, $n = ef$.

Beyond $\mathbb{Q}_p$: finite extensions

Beyond $\mathbb{Q}_p$: finite extensions

Names for Extensions

Names for Extensions

Let K, n, e and f be as before; K is said to be

Names for Extensions

Let K, n, e and f be as before; K is said to be

- **unramified** when $e = 1$, i.e., when $[K : \mathbb{Q}_p] = f$ or p generates $\mathfrak{m}_K$.

Names for Extensions

Let K, n, e and f be as before; K is said to be

- **unramified** when $e = 1$, i.e., when $[K : \mathbb{Q}_p] = f$ or p generates $\mathfrak{m}_K$.
- **totally ramified** when $f = 1$, i.e., when $[K : \mathbb{Q}_p] = e$, or the residue field doesn't grow.

Names for Extensions

Let K, n, e and f be as before; K is said to be

- **unramified** when $e = 1$, i.e., when $[K : \mathbb{Q}_p] = f$ or p generates $\mathfrak{m}_K$.
- **totally ramified** when $f = 1$, i.e., when $[K : \mathbb{Q}_p] = e$, or the residue field doesn't grow.
- **tamely ramified** when $p \nmid e$,

Names for Extensions

Let K, n, e and f be as before; K is said to be

- **unramified** when $e = 1$, i.e., when $[K : \mathbb{Q}_p] = f$ or p generates $\mathfrak{m}_K$.
- **totally ramified** when $f = 1$, i.e., when $[K : \mathbb{Q}_p] = e$, or the residue field doesn't grow.
- **tamely ramified** when $p \nmid e$,
- **wildly ramified** when e is a power of p.

Beyond $\mathbb{Q}_p$: finite extensions

Names for Extensions

Let K, n, e and f be as before; K is said to be

- **unramified** when $e = 1$, i.e., when $[K : \mathbb{Q}_p] = f$ or p generates $\mathfrak{m}_K$.
- **totally ramified** when $f = 1$, i.e., when $[K : \mathbb{Q}_p] = e$, or the residue field doesn't grow.
- **tamely ramified** when $p \nmid e$,
- **wildly ramified** when e is a power of p.

Unramified Extensions

Names for Extensions

Let K, n, e and f be as before; K is said to be

- **unramified** when $e = 1$, i.e., when $[K : \mathbb{Q}_p] = f$ or p generates $\mathfrak{m}_K$.
- **totally ramified** when $f = 1$, i.e., when $[K : \mathbb{Q}_p] = e$, or the residue field doesn't grow.
- **tamely ramified** when $p \nmid e$,
- **wildly ramified** when e is a power of p.

Unramified Extensions

For each f there is exactly one unramified extension of degree f. It can be obtained by adjoining to $\mathbb{Q}_p$ a primitive $(p^f - 1)$-st root of unity.

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}_p}$

The completion of $\overline{\mathbb{Q}_p}$

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$, it is not only completely but also algebraically closed!

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$, it is not only completely but also algebraically closed!

This is the ideal place to do the p-adic version of complex analysis.

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$, it is not only completely but also algebraically closed!

This is the ideal place to do the p-adic version of complex analysis.

The underlying algebraic structure of $\mathbb{C}_p$

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$, it is not only completely but also algebraically closed!

This is the ideal place to do the p-adic version of complex analysis.

The underlying algebraic structure of $\mathbb{C}_p$

$\mathbb{C}_p$ has the cardinality of the continuum.

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$, it is not only completely but also algebraically closed!

This is the ideal place to do the p-adic version of complex analysis.

The underlying algebraic structure of $\mathbb{C}_p$

$\mathbb{C}_p$ has the cardinality of the continuum.

Due to Ernst Steinitz we have the following field theoretic results:

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$, it is not only completely but also algebraically closed!

This is the ideal place to do the p-adic version of complex analysis.

The underlying algebraic structure of $\mathbb{C}_p$

$\mathbb{C}_p$ has the cardinality of the continuum.

Due to Ernst Steinitz we have the following field theoretic results: Two algebraic closures of a field k are k-isomorphic.

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$, it is not only completely but also algebraically closed!

This is the ideal place to do the p-adic version of complex analysis.

The underlying algebraic structure of $\mathbb{C}_p$

$\mathbb{C}_p$ has the cardinality of the continuum.

Due to Ernst Steinitz we have the following field theoretic results: Two algebraic closures of a field k are k-isomorphic. Every field extension K/k has a transcendence basis.

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$, it is not only completely but also algebraically closed!

This is the ideal place to do the p-adic version of complex analysis.

The underlying algebraic structure of $\mathbb{C}_p$

$\mathbb{C}_p$ has the cardinality of the continuum.

Due to Ernst Steinitz we have the following field theoretic results: Two algebraic closures of a field k are k-isomorphic. Every field extension K/k has a transcendence basis. Two transcendence bases K/k have the same cardinality.

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$, it is not only completely but also algebraically closed!

This is the ideal place to do the p-adic version of complex analysis.

The underlying algebraic structure of $\mathbb{C}_p$

$\mathbb{C}_p$ has the cardinality of the continuum.

Due to Ernst Steinitz we have the following field theoretic results: Two algebraic closures of a field k are k-isomorphic. Every field extension K/k has a transcendence basis. Two transcendence bases K/k have the same cardinality.

The result: $\mathbb{C}_p$ and $\mathbb{C}$ are $\mathbb{Q}$-isomorphic.

The analogue of $\mathbb{C}$: completion of $\overline{\mathbb{Q}}_p$

The completion of $\overline{\mathbb{Q}}_p$

We employ the usual process to obtain a metric completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p^{\overline{\mathbb{Q}}_p})$, and $|\cdot|_p^{\overline{\mathbb{Q}}_p})$ lifts to this completion.

The resulting normed field is denoted $\mathbb{C}_p$, it is not only completely but also algebraically closed!

This is the ideal place to do the p-adic version of complex analysis.

The underlying algebraic structure of $\mathbb{C}_p$

$\mathbb{C}_p$ has the cardinality of the continuum.

Due to Ernst Steinitz we have the following field theoretic results: Two algebraic closures of a field k are k-isomorphic. Every field extension K/k has a transcendence basis. Two transcendence bases K/k have the same cardinality.

The result: $\mathbb{C}_p$ and $\mathbb{C}$ are $\mathbb{Q}$-isomorphic. So essentially, $\mathbb{C}_p$ is just $\mathbb{C}$ with a very weird topology.

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$, so just as before, we can consider its "ring of integers"

$$\mathfrak{O} = \{x \in \mathbb{C}_p \mid |x| \leq 1\}$$

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$, so just as before, we can consider its "ring of integers"

$$\mathfrak{O} = \{x \in \mathbb{C}_p \mid |x| \leq 1\}$$

This is again a local ring with maximal ideal

$$\mathfrak{M} = \{x \in \mathbb{C}_p \mid |x| < 1\}$$

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$, so just as before, we can consider its "ring of integers"

$$\mathfrak{O} = \{x \in \mathbb{C}_p \mid |x| \leq 1\}$$

This is again a local ring with maximal ideal

$$\mathfrak{M} = \{x \in \mathbb{C}_p \mid |x| < 1\}$$

The residue field $\mathbb{F} = \mathfrak{O}/\mathfrak{M}$ is an algebraic closure of $\mathbb{F}_p$.

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$, so just as before, we can consider its "ring of integers"

$$\mathfrak{O} = \{x \in \mathbb{C}_p \mid |x| \leq 1\}$$

This is again a local ring with maximal ideal

$$\mathfrak{M} = \{x \in \mathbb{C}_p \mid |x| < 1\}$$

The residue field $\mathbb{F} = \mathfrak{O}/\mathfrak{M}$ is an algebraic closure of $\mathbb{F}_p$.

$\mathbb{C}_p$ is not big enough for functional analysis

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$, so just as before, we can consider its "ring of integers"

$$\mathfrak{O} = \{x \in \mathbb{C}_p \mid |x| \leq 1\}$$

This is again a local ring with maximal ideal

$$\mathfrak{M} = \{x \in \mathbb{C}_p \mid |x| < 1\}$$

The residue field $\mathbb{F} = \mathfrak{O}/\mathfrak{M}$ is an algebraic closure of $\mathbb{F}_p$.

$\mathbb{C}_p$ is not big enough for functional analysis

For the purposes of functional analysis, we want to work over *spherically complete* normed fields

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$, so just as before, we can consider its "ring of integers"

$$\mathfrak{O} = \{x \in \mathbb{C}_p \mid |x| \leq 1\}$$

This is again a local ring with maximal ideal

$$\mathfrak{M} = \{x \in \mathbb{C}_p \mid |x| < 1\}$$

The residue field $\mathbb{F} = \mathfrak{O}/\mathfrak{M}$ is an algebraic closure of $\mathbb{F}_p$.

$\mathbb{C}_p$ is not big enough for functional analysis

For the purposes of functional analysis, we want to work over *spherically complete* normed fields, this a normed field where every nested sequence of closed balls has a non-empty intersection.

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$, so just as before, we can consider its "ring of integers"

$$\mathfrak{O} = \{x \in \mathbb{C}_p \mid |x| \leq 1\}$$

This is again a local ring with maximal ideal

$$\mathfrak{M} = \{x \in \mathbb{C}_p \mid |x| < 1\}$$

The residue field $\mathbb{F} = \mathfrak{O}/\mathfrak{M}$ is an algebraic closure of $\mathbb{F}_p$.

$\mathbb{C}_p$ is not big enough for functional analysis

For the purposes of functional analysis, we want to work over *spherically complete* normed fields, this a normed field where every nested sequence of closed balls has a non-empty intersection. Why haven't you heard of this?

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$, so just as before, we can consider its "ring of integers"

$$\mathfrak{O} = \{x \in \mathbb{C}_p \mid |x| \leq 1\}$$

This is again a local ring with maximal ideal

$$\mathfrak{M} = \{x \in \mathbb{C}_p \mid |x| < 1\}$$

The residue field $\mathbb{F} = \mathfrak{O}/\mathfrak{M}$ is an algebraic closure of $\mathbb{F}_p$.

$\mathbb{C}_p$ is not big enough for functional analysis

For the purposes of functional analysis, we want to work over *spherically complete* normed fields, this a normed field where every nested sequence of closed balls has a non-empty intersection. Why haven't you heard of this? Well, $\mathbb{C}$ is spherically complete.

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$, so just as before, we can consider its "ring of integers"

$$\mathfrak{O} = \{x \in \mathbb{C}_p \mid |x| \leq 1\}$$

This is again a local ring with maximal ideal

$$\mathfrak{M} = \{x \in \mathbb{C}_p \mid |x| < 1\}$$

The residue field $\mathbb{F} = \mathfrak{O}/\mathfrak{M}$ is an algebraic closure of $\mathbb{F}_p$.

$\mathbb{C}_p$ is not big enough for functional analysis

For the purposes of functional analysis, we want to work over *spherically complete* normed fields, this a normed field where every nested sequence of closed balls has a non-empty intersection. Why haven't you heard of this? Well, $\mathbb{C}$ is spherically complete. And you guessed it, $\mathbb{C}_p$ is not!

$\mathbb{C}_p$: has rich algebra but not big enough for all of analysis

$\mathbb{C}_p$ and its related algebraic objects

Recall $\mathbb{C}_p$ is equipped with a non-Archimedean norm, let's denote it $|\cdot|$, so just as before, we can consider its "ring of integers"

$$\mathfrak{O} = \{x \in \mathbb{C}_p \mid |x| \leq 1\}$$

This is again a local ring with maximal ideal

$$\mathfrak{M} = \{x \in \mathbb{C}_p \mid |x| < 1\}$$

The residue field $\mathbb{F} = \mathfrak{O}/\mathfrak{M}$ is an algebraic closure of $\mathbb{F}_p$.

$\mathbb{C}_p$ is not big enough for functional analysis

For the purposes of functional analysis, we want to work over *spherically complete* normed fields, this a normed field where every nested sequence of closed balls has a non-empty intersection. Why haven't you heard of this? Well, $\mathbb{C}$ is spherically complete. And you guessed it, $\mathbb{C}_p$ is not! We can spherically complete it, using something called ultrafilters, the resulting normed field is a complete non-Archimedean, spherically complete and algebraically closed field, non-standardly denoted Ω_p.

Another non-Archimedean Field: order of vanishing

Another non-Archimedean Field: order of vanishing

Another non-Archimedean story

Another non-Archimedean Field: order of vanishing

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation v_a.

Another non-Archimedean Field: order of vanishing

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation v_a.
- For any $f \in K[t]$, define $v_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation ν_a.
- For any $f \in K[t]$, define $\nu_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $\nu_a(f/g) \coloneqq \nu_a(f) - \nu_a(g)$.

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation v_a.
- For any $f \in K[t]$, define $v_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $v_a(f/g) \coloneqq v_a(f) - v_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{v_a(f/g)}$ defines a non-Archimedean norm.

Another non-Archimedean Field: order of vanishing

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation ν_a.
- For any $f \in K[t]$, define $\nu_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $\nu_a(f/g) \coloneqq \nu_a(f) - \nu_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{\nu_a(f/g)}$ defines a non-Archimedean norm.
- Completion of $K(t)$ is $K((t-a))$, the field of Laurent series centered at a.

Another non-Archimedean Field: order of vanishing

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation v_a.
- For any $f \in K[t]$, define $v_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $v_a(f/g) \coloneqq v_a(f) - v_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{v_a(f/g)}$ defines a non-Archimedean norm.
- Completion of $K(t)$ is $K((t-a))$, the field of Laurent series centered at a.
- Its valuation ring is $K[[t-a]]$, the ring of Taylor series centered at a.

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation ν_a.
- For any $f \in K[t]$, define $\nu_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $\nu_a(f/g) \coloneqq \nu_a(f) - \nu_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{\nu_a(f/g)}$ defines a non-Archimedean norm.
- Completion of $K(t)$ is $K((t-a))$, the field of Laurent series centered at a.
- Its valuation ring is $K[[t-a]]$, the ring of Taylor series centered at a.
- If $\operatorname{char} K = 0$, an algebraic closure of $K[[t-a]]$ is $K\{\{t-a\}\}$; it's the field of Puiseux series.

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation ν_a.
- For any $f \in K[t]$, define $\nu_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $\nu_a(f/g) \coloneqq \nu_a(f) - \nu_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{\nu_a(f/g)}$ defines a non-Archimedean norm.
- Completion of $K(t)$ is $K((t-a))$, the field of Laurent series centered at a.
- Its valuation ring is $K[[t-a]]$, the ring of Taylor series centered at a.
- If $\operatorname{char} K = 0$, an algebraic closure of $K[[t-a]]$ is $K\{\{t-a\}\}$; it's the field of Puiseux series.
- The completion of the field of Puiseux series is the Levi-Civita field.

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation ν_a.
- For any $f \in K[t]$, define $\nu_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $\nu_a(f/g) \coloneqq \nu_a(f) - \nu_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{\nu_a(f/g)}$ defines a non-Archimedean norm.
- Completion of $K(t)$ is $K((t-a))$, the field of Laurent series centered at a.
- Its valuation ring is $K[[t-a]]$, the ring of Taylor series centered at a.
- If $\operatorname{char} K = 0$, an algebraic closure of $K[[t-a]]$ is $K\{\{t-a\}\}$; it's the field of Puiseux series.
- The completion of the field of Puiseux series is the Levi-Civita field.
- An important example: characteristic p analogue of $\mathbb{Q}_p$ is $\mathbb{F}_q((t))$.

Another non-Archimedean Field: order of vanishing

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation v_a.
- For any $f \in K[t]$, define $v_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $v_a(f/g) \coloneqq v_a(f) - v_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{v_a(f/g)}$ defines a non-Archimedean norm.
- Completion of $K(t)$ is $K((t-a))$, the field of Laurent series centered at a.
- Its valuation ring is $K[[t-a]]$, the ring of Taylor series centered at a.
- If $\operatorname{char} K = 0$, an algebraic closure of $K[[t-a]]$ is $K\{\{t-a\}\}$; it's the field of Puiseux series.
- The completion of the field of Puiseux series is the Levi-Civita field.
- An important example: characteristic p analogue of $\mathbb{Q}_p$ is $\mathbb{F}_q((t))$.

  It is not just an ultrametric space but also a local field (locally compact as a topological field).

Another non-Archimedean Field: order of vanishing

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation ν_a.
- For any $f \in K[t]$, define $\nu_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $\nu_a(f/g) \coloneqq \nu_a(f) - \nu_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{\nu_a(f/g)}$ defines a non-Archimedean norm.
- Completion of $K(t)$ is $K((t-a))$, the field of Laurent series centered at a.
- Its valuation ring is $K[[t-a]]$, the ring of Taylor series centered at a.
- If char $K = 0$, an algebraic closure of $K[[t-a]]$ is $K\{\{t-a\}\}$; it's the field of Puiseux series.
- The completion of the field of Puiseux series is the Levi-Civita field.
- An important example: characteristic p analogue of $\mathbb{Q}_p$ is $\mathbb{F}_q((t))$.

  It is not just an ultrametric space but also a local field (locally compact as a topological field).

  There's a complete classification (upto isomorphism of topological fields) of local fields

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation ν_a.
- For any $f \in K[t]$, define $\nu_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $\nu_a(f/g) \coloneqq \nu_a(f) - \nu_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{\nu_a(f/g)}$ defines a non-Archimedean norm.
- Completion of $K(t)$ is $K((t-a))$, the field of Laurent series centered at a.
- Its valuation ring is $K[[t-a]]$, the ring of Taylor series centered at a.
- If char $K = 0$, an algebraic closure of $K[[t-a]]$ is $K\{\{t-a\}\}$; it's the field of Puiseux series.
- The completion of the field of Puiseux series is the Levi-Civita field.
- An important example: characteristic p analogue of $\mathbb{Q}_p$ is $\mathbb{F}_q((t))$.

  It is not just an ultrametric space but also a local field (locally compact as a topological field).

  There's a complete classification (upto isomorphism of topological fields) of local fields:
  if Archimedean, then $\mathbb{R}$ or $\mathbb{C}$;

Another non-Archimedean Field: order of vanishing

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation ν_a.
- For any $f \in K[t]$, define $\nu_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $\nu_a(f/g) \coloneqq \nu_a(f) - \nu_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{\nu_a(f/g)}$ defines a non-Archimedean norm.
- Completion of $K(t)$ is $K((t-a))$, the field of Laurent series centered at a.
- Its valuation ring is $K[[t-a]]$, the ring of Taylor series centered at a.
- If $\operatorname{char} K = 0$, an algebraic closure of $K[[t-a]]$ is $K\{\{t-a\}\}$; it's the field of Puiseux series.
- The completion of the field of Puiseux series is the Levi-Civita field.
- An important example: characteristic p analogue of $\mathbb{Q}_p$ is $\mathbb{F}_q((t))$.

  It is not just an ultrametric space but also a local field (locally compact as a topological field).

  There's a complete classification (upto isomorphism of topological fields) of local fields:
  if Archimedean, then $\mathbb{R}$ or $\mathbb{C}$; if non-Archimedean of characteristic 0, then a finite extension of $\mathbb{Q}_p$;

Another non-Archimedean story

Fix any field K, and consider the ring of rational functions $K(t)$, and fix some $a \in K$

- We introduce the order of vanishing valuation ν_a.
- For any $f \in K[t]$, define $\nu_a(f) \coloneqq k$, if $(t-a)^k \parallel f$.
- For $f/g \in K(t)$, define $\nu_a(f/g) \coloneqq \nu_a(f) - \nu_a(g)$.
- $|f/g|_{t-a} \coloneqq (t-a)^{\nu_a(f/g)}$ defines a non-Archimedean norm.
- Completion of $K(t)$ is $K((t-a))$, the field of Laurent series centered at a.
- Its valuation ring is $K[[t-a]]$, the ring of Taylor series centered at a.
- If char $K = 0$, an algebraic closure of $K[[t-a]]$ is $K\{\{t-a\}\}$; it's the field of Puiseux series.
- The completion of the field of Puiseux series is the Levi-Civita field.
- An important example: characteristic p analogue of $\mathbb{Q}_p$ is $\mathbb{F}_q((t))$.

  It is not just an ultrametric space but also a local field (locally compact as a topological field).

  There's a complete classification (upto isomorphism of topological fields) of local fields:
  if Archimedean, then $\mathbb{R}$ or $\mathbb{C}$; if non-Archimedean of characteristic 0, then a finite extension of $\mathbb{Q}_p$;
  if non-Archimedean of characteristic p, then a finite extension of $\mathbb{F}_q((t))$.

Fin.

References

[1] Robert, A. M. (2000). *A Course in p-adic Analysis*. New York: Springer.

[2] Gouvêa, F. Q. (2020). *p-adic Numbers: an introduction*. Springer Nature.

[3] Koblitz, N. (1984). *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. New York: Springer.

[4] Schikhof, W. H. (2006). *Ultrametric calculus: an introduction to p-adic analysis*. Cambridge: Cambridge Univ. Press.

[5] Serre, J.-P. (1973). *A course in arithmetic*. New York, Heidelberg, Berlin: Springer.

[6] Murty, M. R. (2002). *Introduction to p-adic analytic number theory*. Providence, RI: American Mathematical Society.

[7] Katok, Svetlana (2007). *p-adic analysis compared with real*. Providence, RI: American Mathematical Society.

[8] Milne, J. S. (2020). *Algebraic Number Theory (v3.08)*. Available at `https://www.jmilne.org/math/`. Accessed 06 November 2020