p-Adic Numbers and Krasner's Lemma

Jonatan Beiruty and Alois Schaffler

May 22, 2025

Plan for Today

- 1. Construction of p-adic numbers and their properties.
- 2. Reminder of field theory and Krasner's lemma.
- 3. Krasner's lemma in Lean.
- 4. Lean implementation and main takeaways.

Norms and Induced Metrics

Let K be a field. A function $\|\cdot\| : K \to \mathbb{R}_{\geq 0}$ is called a **norm** (or absolute value) on K if it satisfies, for all $x, y \in K$:

- **Non-degeneracy:** $\|x\| = 0 \iff x = 0$,
- **Multiplicativity:** $\|xy\| = \|x\| \cdot \|y\|$,
- **Triangle inequality:** $\|x + y\| \leq \|x\| + \|y\|$.

Norms and Induced Metrics

Let K be a field. A function $\|\cdot\| : K \to \mathbb{R}_{\geq 0}$ is called a **norm** (or absolute value) on K if it satisfies, for all $x, y \in K$:

- **Non-degeneracy:** $\|x\| = 0 \iff x = 0$,
- **Multiplicativity:** $\|xy\| = \|x\| \cdot \|y\|$,
- **Triangle inequality:** $\|x + y\| \leq \|x\| + \|y\|$.

A norm is called **non-Archimedean** if

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

The p-Adic Norm on $\mathbb{Q}$

Let p be a fixed prime number. Define

$$\mathrm{ord}_p(n) := \max\{k \in \mathbb{Z}_{\geq 0} \mid p^k \mid n\}.$$

The p-Adic Norm on $\mathbb{Q}$

Let p be a fixed prime number. Define

$$\operatorname{ord}_p(n) := \max\{k \in \mathbb{Z}_{\geq 0} \mid p^k \mid n\}.$$

This extends naturally to nonzero rationals:

$$\operatorname{ord}_p\left(\frac{a}{b}\right) := \operatorname{ord}_p(a) - \operatorname{ord}_p(b).$$

The p-Adic Norm on $\mathbb{Q}$

Let p be a fixed prime number. Define

$$\operatorname{ord}_p(n) := \max\{k \in \mathbb{Z}_{\geq 0} \mid p^k \mid n\}.$$

This extends naturally to nonzero rationals:

$$\operatorname{ord}_p\left(\frac{a}{b}\right) := \operatorname{ord}_p(a) - \operatorname{ord}_p(b).$$

The p-**adic norm** on $\mathbb{Q}$ is then defined as:

$$|x|_p := \begin{cases} p^{-\operatorname{ord}_p(x)} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

This is a non-Archimedean norm.

Examples

- $|27|_3 = 3^{-\operatorname{ord}_3(27)} = 3^{-3} = \frac{1}{27}$,
- $\left|\frac{81}{2}\right|_3 = 3^{-(\operatorname{ord}_3(81) - \operatorname{ord}_3(2)} = 3^{-4} = \frac{1}{81}$,
- $\left|\frac{1}{243}\right|_3 = 3^{-(\operatorname{ord}_3(1) - \operatorname{ord}_3(243))} = 3^5 = 243$.

Examples

- $|27|_3 = 3^{-\operatorname{ord}_3(27)} = 3^{-3} = \frac{1}{27}$,
- $\left|\frac{81}{2}\right|_3 = 3^{-(\operatorname{ord}_3(81) - \operatorname{ord}_3(2)} = 3^{-4} = \frac{1}{81}$,
- $\left|\frac{1}{243}\right|_3 = 3^{-(\operatorname{ord}_3(1) - \operatorname{ord}_3(243))} = 3^5 = 243.$

Observation: The *p*-adic concept of size is very different from our usual understanding.

Ostrowski's Theorem

Theorem: Every absolute value $\|\cdot\|$ on $\mathbb{Q}$ is equivalent to exactly one of the following:

- The trivial absolute value, given by $\|x\|_{\mathrm{triv}} = 1$ for $x \neq 0$.
- The usual absolute value $|\cdot|$.
- A p-adic norm $|\cdot|_p$ for some prime p.

Completeness

Recall that a metric space is called complete if every Cauchy sequence is convergent. Completeness is one of the most fundamental properties of metric spaces.

Completeness

Recall that a metric space is called complete if every Cauchy sequence is convergent. Completeness is one of the most fundamental properties of metric spaces.

The space $(\mathbb{Q}, |\cdot|_p)$ is not complete. Its **completion** is denoted $\mathbb{Q}_p$, the ***p*-adic numbers**.

Completion of $(\mathbb{Q}, |\cdot|_p)$

We will construct a normed field $(\mathbb{Q}_p, |\cdot|_p)$ satisfying the following properties:

Completion of $(\mathbb{Q}, |\cdot|_p)$

We will construct a normed field $(\mathbb{Q}_p, |\cdot|_p)$ satisfying the following properties:

- $(\mathbb{Q}_p, |\cdot|_p)$ is complete.

Completion of $(\mathbb{Q}, |\cdot|_p)$

We will construct a normed field $(\mathbb{Q}_p, |\cdot|_p)$ satisfying the following properties:

- $(\mathbb{Q}_p, |\cdot|_p)$ is complete.
- There is an embedding $\iota\colon \mathbb{Q} \to \mathbb{Q}_p$.

Completion of $(\mathbb{Q}, |\cdot|_p)$

We will construct a normed field $(\mathbb{Q}_p, |\cdot|_p)$ satisfying the following properties:

- $(\mathbb{Q}_p, |\cdot|_p)$ is complete.
- There is an embedding $\iota\colon \mathbb{Q} \to \mathbb{Q}_p$.
- $\iota(\mathbb{Q})$ is dense in $\mathbb{Q}_p$.

Completion of $(\mathbb{Q}, |\cdot|_p)$

We will construct a normed field $(\mathbb{Q}_p, |\cdot|_p)$ satisfying the following properties:

- $(\mathbb{Q}_p, |\cdot|_p)$ is complete.
- There is an embedding $\iota\colon \mathbb{Q} \to \mathbb{Q}_p$.
- $\iota(\mathbb{Q})$ is dense in $\mathbb{Q}_p$.
- ι is an isometry, that is $|\iota(x)|_p = |x|_p$ for all $x \in \mathbb{Q}$.

Construction of $\mathbb{Q}_p$

Step 1: Consider the set of all Cauchy sequences in $(\mathbb{Q}, |\cdot|_p)$:

$$\mathcal{C}_p := \{(a_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} \mid (a_n)_{n\in\mathbb{N}} \text{ is a Cauchy sequence } \}.$$

Construction of $\mathbb{Q}_p$

Step 1: Consider the set of all Cauchy sequences in $(\mathbb{Q}, |\cdot|_p)$:

$$\mathcal{C}_p := \{(a_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} \mid (a_n)_{n\in\mathbb{N}} \text{ is a Cauchy sequence } \}.$$

Step 2: Define the following equivalence relation:

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

Construction of $\mathbb{Q}_p$

Step 1: Consider the set of all Cauchy sequences in $(\mathbb{Q}, |\cdot|_p)$:

$$\mathcal{C}_p := \{(a_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} \mid (a_n)_{n\in\mathbb{N}} \text{ is a Cauchy sequence } \}.$$

Step 2: Define the following equivalence relation:

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

Step 3: Define the p-adic numbers as

$$\mathbb{Q}_p := \mathcal{C}_p / \sim .$$

Construction of $\mathbb{Q}_p$

Step 1: Consider the set of all Cauchy sequences in $(\mathbb{Q}, |\cdot|_p)$:

$$\mathcal{C}_p := \{(a_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} \mid (a_n)_{n\in\mathbb{N}} \text{ is a Cauchy sequence } \}.$$

Step 2: Define the following equivalence relation:

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

Step 3: Define the p-adic numbers as

$$\mathbb{Q}_p := \mathcal{C}_p / \sim .$$

Defining the norm on $\mathbb{Q}_p$: For a class $[(a_n)_{n\in\mathbb{N}}] \in \mathbb{Q}_p$, define:

$$|[(a_n)_{n\in\mathbb{N}}]|_p := \lim_{n\to\infty} |a_n|_p$$

Construction of $\mathbb{Q}_p$

Operations on $\mathbb{Q}_p$:

$$[(a_n)_{n\in\mathbb{N}}] + [(b_n)_{n\in\mathbb{N}}] := [(a_n + b_n)_{n\in\mathbb{N}}],$$
$$[(a_n)_{n\in\mathbb{N}}][(b_n)_{n\in\mathbb{N}}] := [(a_n b_n)_{n\in\mathbb{N}}].$$

Construction of $\mathbb{Q}_p$

Operations on $\mathbb{Q}_p$:

$$[(a_n)_{n\in\mathbb{N}}] + [(b_n)_{n\in\mathbb{N}}] := [(a_n + b_n)_{n\in\mathbb{N}}],$$
$$[(a_n)_{n\in\mathbb{N}}][(b_n)_{n\in\mathbb{N}}] := [(a_n b_n)_{n\in\mathbb{N}}].$$

We define

$$\begin{aligned} \iota \colon \mathbb{Q} &\to \mathbb{Q}_p \\ x &\mapsto [(x)_{n\in\mathbb{N}}]. \end{aligned}$$

Construction of $\mathbb{Q}_p$

Operations on $\mathbb{Q}_p$:

$$[(a_n)_{n\in\mathbb{N}}] + [(b_n)_{n\in\mathbb{N}}] := [(a_n + b_n)_{n\in\mathbb{N}}],$$
$$[(a_n)_{n\in\mathbb{N}}][(b_n)_{n\in\mathbb{N}}] := [(a_n b_n)_{n\in\mathbb{N}}].$$

We define

$$\begin{aligned} \iota\colon \mathbb{Q} &\to \mathbb{Q}_p \\ x &\mapsto [(x)_{n\in\mathbb{N}}]. \end{aligned}$$

All of these definitions are well-defined, which is checked by routine arguments, and our desired properties are fulfilled.

Properties of $\mathbb{Q}_p$

- $(\mathbb{Q}_p, |\cdot|_p)$ is complete.

Properties of $\mathbb{Q}_p$

- $(\mathbb{Q}_p, |\cdot|_p)$ is complete.
- The norm $|\cdot|_p$ on $\mathbb{Q}_p$ is non-Archimedian.

Properties of $\mathbb{Q}_p$

- $(\mathbb{Q}_p, |\cdot|_p)$ is complete.
- The norm $|\cdot|_p$ on $\mathbb{Q}_p$ is non-Archimedian.
- The values of $|\cdot|_p$ lie in the set

$$\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}.$$

Properties of $\mathbb{Q}_p$

- $(\mathbb{Q}_p, |\cdot|_p)$ is complete.
- The norm $|\cdot|_p$ on $\mathbb{Q}_p$ is non-Archimedian.
- The values of $|\cdot|_p$ lie in the set

$$\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}.$$

- $\mathbb{Q}_p$ is totally disconnected.

Properties of $\mathbb{Q}_p$

- $(\mathbb{Q}_p, |\cdot|_p)$ is complete.
- The norm $|\cdot|_p$ on $\mathbb{Q}_p$ is non-Archimedian.
- The values of $|\cdot|_p$ lie in the set

$$\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}.$$

- $\mathbb{Q}_p$ is totally disconnected.
- $\mathbb{Q}_p$ is locally compact.

Properties of $\mathbb{Q}_p$

- $(\mathbb{Q}_p, |\cdot|_p)$ is complete.
- The norm $|\cdot|_p$ on $\mathbb{Q}_p$ is non-Archimedian.
- The values of $|\cdot|_p$ lie in the set

$$\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}.$$

- $\mathbb{Q}_p$ is totally disconnected.
- $\mathbb{Q}_p$ is locally compact.
- $\mathbb{Q}_p$ is **not** algebraically closed.

Algebraic Closure and Completeness

We would like to have an algebraically closed and complete field containing $\mathbb{Q}$. Consider the algebraic closure $\overline{\mathbb{Q}_p}$. It is possible to extend $|\cdot|_p$ to $\overline{\mathbb{Q}_p}$.

Algebraic Closure and Completeness

We would like to have an algebraically closed and complete field containing $\mathbb{Q}$. Consider the algebraic closure $\overline{\mathbb{Q}_p}$. It is possible to extend $|\cdot|_p$ to $\overline{\mathbb{Q}_p}$. However, $(\overline{\mathbb{Q}_p}, |\cdot|_p)$ is not complete.

Algebraic Closure and Completeness

We would like to have an algebraically closed and complete field containing $\mathbb{Q}$. Consider the algebraic closure $\overline{\mathbb{Q}_p}$. It is possible to extend $|\cdot|_p$ to $\overline{\mathbb{Q}_p}$. However, $(\overline{\mathbb{Q}_p}, |\cdot|_p)$ is not complete.

Question: In the p-adic world, can we ever reach a field that is *both* complete and algebraically closed?

Algebraic Closure and Completeness

We would like to have an algebraically closed and complete field containing $\mathbb{Q}$. Consider the algebraic closure $\overline{\mathbb{Q}_p}$. It is possible to extend $|\cdot|_p$ to $\overline{\mathbb{Q}_p}$. However, $(\overline{\mathbb{Q}_p}, |\cdot|_p)$ is not complete.

Question: In the p-adic world, can we ever reach a field that is *both* complete and algebraically closed?

Answer: Yes, we can. Completing $(\overline{\mathbb{Q}_p}, |\cdot|_p)$ yields a non-Archimedean normed field $(\mathbb{C}_p, |\cdot|_p)$ which is complete and algebraically closed.

3-adic Visualization Animation

Some Field Theory

Let L/K be a field extension, meaning that K is a subfield of L.

Some Field Theory

Let L/K be a field extension, meaning that K is a subfield of L.

- An element $x \in L$ is called **algebraic** over K if there exists a non-zero polynomial $P \in K[X]$ with $P(x) = 0$.

Some Field Theory

Let L/K be a field extension, meaning that K is a subfield of L.

- An element $x \in L$ is called **algebraic** over K if there exists a non-zero polynomial $P \in K[X]$ with $P(x) = 0$.
- The **minimal polynomial** $P_x \in K[X]$ of an algebraic element is the unique monic irreducible polynomial in $K[X]$ with $P_x(x) = 0$.

Some Field Theory

Let L/K be a field extension, meaning that K is a subfield of L.

- An element $x \in L$ is called **algebraic** over K if there exists a non-zero polynomial $P \in K[X]$ with $P(x) = 0$.
- The **minimal polynomial** $P_x \in K[X]$ of an algebraic element is the unique monic irreducible polynomial in $K[X]$ with $P_x(x) = 0$.
- The extension L/K is called algebraic if every element of L is algebraic over K.

Some Field Theory

Let L/K be a field extension, meaning that K is a subfield of L.

- An element $x \in L$ is called **algebraic** over K if there exists a non-zero polynomial $P \in K[X]$ with $P(x) = 0$.
- The **minimal polynomial** $P_x \in K[X]$ of an algebraic element is the unique monic irreducible polynomial in $K[X]$ with $P_x(x) = 0$.
- The extension L/K is called algebraic if every element of L is algebraic over K.
- Suppose that the minimal polynomial P_x of $x \in L$ splits as a product of linear factors in $L[X]$. The **conjugates** of x over K are the zeros of P_x in L.

Some Field Theory

Let L/K be a field extension, meaning that K is a subfield of L.

- An element $x \in L$ is called **algebraic** over K if there exists a non-zero polynomial $P \in K[X]$ with $P(x) = 0$.
- The **minimal polynomial** $P_x \in K[X]$ of an algebraic element is the unique monic irreducible polynomial in $K[X]$ with $P_x(x) = 0$.
- The extension L/K is called algebraic if every element of L is algebraic over K.
- Suppose that the minimal polynomial P_x of $x \in L$ splits as a product of linear factors in $L[X]$. The **conjugates** of x over K are the zeros of P_x in L.
- An algebraic element $x \in L$ is called **separable** if the minimal polynomial $P_x \in K[X]$ only has simple roots (in some field where it splits).

Some Field Theory

Let L/K be a field extension, meaning that K is a subfield of L.

- An element $x \in L$ is called **algebraic** over K if there exists a non-zero polynomial $P \in K[X]$ with $P(x) = 0$.
- The **minimal polynomial** $P_x \in K[X]$ of an algebraic element is the unique monic irreducible polynomial in $K[X]$ with $P_x(x) = 0$.
- The extension L/K is called algebraic if every element of L is algebraic over K.
- Suppose that the minimal polynomial P_x of $x \in L$ splits as a product of linear factors in $L[X]$. The **conjugates** of x over K are the zeros of P_x in L.
- An algebraic element $x \in L$ is called **separable** if the minimal polynomial $P_x \in K[X]$ only has simple roots (in some field where it splits).
- We denote $K(x)$ the smallest subfield of L containing $K \cup \{x\}$.

Krasner's Lemma

Theorem: Let $a, b \in \overline{\mathbb{Q}_p}$. Suppose that for every conjugate $a_i \neq a$ of a in $\overline{\mathbb{Q}_p}$ (over $\mathbb{Q}_p$) it holds that

$$|b-a|_p < |a_i - a|_p.$$

Then $\mathbb{Q}_p(a) \subseteq \mathbb{Q}_p(b)$.

Krasner's Lemma

Theorem: Let $a, b \in \overline{\mathbb{Q}_p}$. Suppose that for every conjugate $a_i \neq a$ of a in $\overline{\mathbb{Q}_p}$ (over $\mathbb{Q}_p$) it holds that

$$|b - a|_p < |a_i - a|_p.$$

Then $\mathbb{Q}_p(a) \subseteq \mathbb{Q}_p(b)$.

Krasner's lemma can be used to prove that $\mathbb{C}_p$ is algebraically closed.

Proof of Krasner's Lemma

Set $K := \mathbb{Q}_p(b)$, and assume by way of contradiction that $a \notin K$.

Proof of Krasner's Lemma

Set $K := \mathbb{Q}_p(b)$, and assume by way of contradiction that $a \notin K$. By basic results from field theory, it follows that there exists a conjugate $a_i \neq a$ of a over K.

Proof of Krasner's Lemma

Set $K := \mathbb{Q}_p(b)$, and assume by way of contradiction that $a \notin K$. By basic results from field theory, it follows that there exists a conjugate $a_i \neq a$ of a over K. Again by field theory, there exists an isomorphism

$$\sigma \colon K(a) \to K(a_i)$$

such that $\sigma|_K = \mathrm{id}_K$ and $\sigma(a) = a_i$.

Proof of Krasner's Lemma

Set $K := \mathbb{Q}_p(b)$, and assume by way of contradiction that $a \notin K$. By basic results from field theory, it follows that there exists a conjugate $a_i \neq a$ of a over K. Again by field theory, there exists an isomorphism

$$\sigma \colon K(a) \to K(a_i)$$

such that $\sigma|_K = \mathrm{id}_K$ and $\sigma(a) = a_i$. We will see later that $|\cdot|_p$ is invariant under isomorphisms, i.e. $|\sigma(x)|_p = |x|_p$ for every $x \in K(a)$.

Proof of Krasner's Lemma

This implies that

$$|b - a|_p = |\sigma(b - a)|_p = |b - \sigma(a)|_p = |b - a_i|_p.$$

Proof of Krasner's Lemma

This implies that

$$|b-a|_p = |\sigma(b-a)|_p = |b-\sigma(a)|_p = |b-a_i|_p.$$

We conclude that

$$\begin{aligned} |a_i-a|_p &= |a_i-b+b-a|_p \leq \max\{|a_i-b|_p, |b-a|_p\} \\ &= |b-a|_p < |a_i-a|_p, \end{aligned}$$

which is a contradiction.

Implementation in Lean

Some More Field Theory

Let L/K be a finite (hence also algebraic) field extension.

- For $x \in L$, denote $m_x \colon L \to L$ to be the K-linear map of multiplication by x.

Some More Field Theory

Let L/K be a finite (hence also algebraic) field extension.

- For $x \in L$, denote $m_x \colon L \to L$ to be the K-linear map of multiplication by x.
- We define the norm of x as $N_{L/K}(x) = \det(m_x)$.

Some More Field Theory

Let L/K be a finite (hence also algebraic) field extension.

- For $x \in L$, denote $m_x \colon L \to L$ to be the K-linear map of multiplication by x.
- We define the norm of x as $N_{L/K}(x) = \det(m_x)$.
- It holds that $N_{L/K}(x) \in K$ and $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.

Some More Field Theory

Let L/K be a finite (hence also algebraic) field extension.

- For $x \in L$, denote $m_x \colon L \to L$ to be the K-linear map of multiplication by x.
- We define the norm of x as $N_{L/K}(x) = \det(m_x)$.
- It holds that $N_{L/K}(x) \in K$ and $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.
- For $x \in K$, we have that $N_{L/K}(x) = x^{[L:K]}$.

Some More Field Theory

Let L/K be a finite (hence also algebraic) field extension.

- For $x \in L$, denote $m_x \colon L \to L$ to be the K-linear map of multiplication by x.
- We define the norm of x as $N_{L/K}(x) = \det(m_x)$.
- It holds that $N_{L/K}(x) \in K$ and $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.
- For $x \in K$, we have that $N_{L/K}(x) = x^{[L:K]}$.
- If M/L is another finite field extension, then $N_{M/K} = N_{L/K} \circ N_{M/L}$.

Extension of Norms

Let L/K be a finite field extension and suppose that K is a normed field.

Extension of Norms

Let L/K be a finite field extension and suppose that K is a normed field.We define a norm an L that extends the norm on K via

$$\|x\| = \|N_{L/K}(x)\|^{1/[L:K]}.$$

Extension of Norms

Let L/K be a finite field extension and suppose that K is a normed field.We define a norm an L that extends the norm on K via

$$\|x\| = \|N_{L/K}(x)\|^{1/[L:K]}.$$

If M is an intermediate field of L/K containing x, then

$$\begin{aligned}\|N_{L/K}(x)\|^{1/[L:K]} &= \|N_{M/K}(N_{L/M}(x)\|^{1/[L:K]} \\ &= \|N_{M/K}(x)\|^{[L:M]/[L:K]} = \|N_{M/K}(x)\|^{1/[M:K]}.\end{aligned}$$

Extension of Norms

Let L/K be a finite field extension and suppose that K is a normed field.We define a norm an L that extends the norm on K via

$$\|x\| = \|N_{L/K}(x)\|^{1/[L:K]}.$$

If M is an intermediate field of L/K containing x, then

$$\begin{aligned}\|N_{L/K}(x)\|^{1/[L:K]} &= \|N_{M/K}(N_{L/M}(x)\|^{1/[L:K]} \\ &= \|N_{M/K}(x)\|^{[L:M]/[L:K]} = \|N_{M/K}(x)\|^{1/[M:K]}.\end{aligned}$$

Hence we can extend the norm on K to a norm on the algebraic closure $\bar{K}$.

Extension of Norms

- Showing that the triangle inequality holds is not so easy.

Extension of Norms

- Showing that the triangle inequality holds is not so easy.
- If K is complete, then this extension is unique.

Extension of Norms

- Showing that the triangle inequality holds is not so easy.
- If K is complete, then this extension is unique.
- If K is complete, non-Archimedian and locally compact, the extended norm is also non-Archimedian. Again, the non-Archimedian triangle inequality is a little tricky to check.

Krasner's Lemma in Lean

```
theorem lemma_krasner {p : ℕ} [Fact (Nat.Prime p)] (a b : AlgebraicClosure ℚ_p)
(h : ∀x ∈ AlgebraicClosure ℚ_p, x ≠ a ∧ IsConjRoot ℚ_p a x →
PAdicNormExt(b − a) < PAdicNormExt(x − a)) :
adjoin ℚ_p ({a} : Set (AlgebraicClosure ℚ_p)) adjoin ℚ_p ({b} : Set
(AlgebraicClosure ℚ_p)) :=
```

Lean	**Explanation**
`have ha : a adjoin Q_p ({b} : Set (AlgebraicClosure Q_p)) := lemma_main a b h`	*We prove that a belongs to K(b) using the 'main_lemma'*
`adjoin_of_mem_adjoin a b ha`	*We explain why it's enough to deduce that there is field embedding of K(a) to K(b)*

Main Lemma in Lean

lemma lemma_main $\{p : \mathbb{N}\}$ [Fact (Nat.Prime p)] (a b : AlgebraicClosure $\mathbb{Q}_p$)
(h : $\forall x \in$ AlgebraicClosure $\mathbb{Q}_p$, $a \neq x \wedge$ IsConjRoot $\mathbb{Q}_p$ a $x \to$
PAdicNormExt($b - a$) $<$ PAdicNormExt($x - a$)) :
$a \in$ adjoin ℚ_p ({b} : Set (AlgebraicClosure ℚ_p)) :=

Lean	Explanation
`have h1 :   (c : AlgebraicClosure Q_p), a  c  IsConjRoot K a c := conj_lemma K a h0`	*Get a Galois conj.*
`have h2 :   ( : AlgebraicClosure Q_p [K] AlgebraicClosure Q_p), a = c   x  K,  x = x := sigma_isom K a c h_conj_in_K`	*Get an isom. from the conj.*

Norm Invariance

```
have h4 : PAdicNormExt (b - a) = PAdicNormExt (c - b) := calc
```

PAdicNormExt (b - a) = PAdicNormExt (σ (b - a)) := h_norm_inv	*Norm invariance*
= PAdicNormExt (σ b - σ a) := Lin_of_sigma	*Linearity*
= PAdicNormExt (b - σ a) := by rw [sigma_b]	*b is fixed*
= PAdicNormExt (b - c) := by rw [h_sigma1]	*a is sent to c*
= PAdicNormExt (-(b - c)) := PAdicNormExt_mult_minus (b - c)	*Norm inv -1*
= PAdicNormExt (c - b) := neg_sub_norm	*Norm sym.*

Contradiction Step

```
have h5 : PAdicNormExt (c - a) < PAdicNormExt (c - a) := calc
```

PAdicNormExt (c - a) = PAdicNormExt ((c - b) + (b - a)) := by rw [sub_add_sub_cancel]	*Add and subtract*
_ ≤ max (PAdicNormExt (c - b)) (PAdicNormExt (b - a)) := PAdicNormExt_non_arch (c - b) (b - a)	*Non-arch triangle ineq.*
= PAdicNormExt (b - a) := max_is_b_sub_a	*By h4*
< PAdicNormExt (c - a) := h c a_c_IsConj_in_Q_p	*Our assumption*

Implementation in Lean – Key Points and Takeaways

- Many parts of this were already implemented in Lean 3 (approx. 5000 lines of code), but the PR was never merged.
- **Intermediate fields:** Sometimes it's best to work under a much bigger field than you "need" to avoid complications from type mismatches and coercions.
- The norm extension over $\mathbb{Q}_p$.