The p-adic numbers: what they are and what they are good for

Browsing Through Mathematics

Andrea Mori

Department of Mathematics
University of Torino

April 28th, 2014

The natural numbers $\mathbb{N}$

Basically all mathematics deals or uses **numbers** and their properties. The most basic set of numbers is the set of **natural numbers**

$$\mathbb{N} = \{0, 1, 2, \ldots\}.$$

After failed attempts to construct $\mathbb{N}$ from simpler set-theoretic entities, it was finally resolved to define it axiomatically. E.g. **Peano axioms (1889):**

P1 $\exists\ 0 \in \mathbb{N}$.

P2 $\exists$ injective function $\sigma : \mathbb{N} \to \mathbb{N}$ s.t. $\sigma(n) \neq 0, \forall n \in \mathbb{N}$.

P3 **(Induction principle)** If $A \subseteq \mathbb{N}$ is s.t. $0 \in A$ and $\forall n \in A, \sigma(n) \in A$ then $A = \mathbb{N}$.

The axioms allow to define **addition** and **multiplication** in $\mathbb{N}$.

The natural numbers $\mathbb{N}$

Basically all mathematics deals or uses **numbers** and their properties. The most basic set of numbers is the set of **natural numbers**

$$\mathbb{N} = \{0, 1, 2, \ldots\}.$$

After failed attempts to construct $\mathbb{N}$ from simpler set-theoretic entities, it was finally resolved to define it axiomatically. E.g. **Peano axioms (1889):**

- P1 $\exists\ 0 \in \mathbb{N}$.
- P2 $\exists$ injective function $\sigma : \mathbb{N} \to \mathbb{N}$ s.t. $\sigma(n) \neq 0, \forall n \in \mathbb{N}$.
- P3 **(Induction principle)** If $A \subseteq \mathbb{N}$ is s.t. $0 \in A$ and $\forall n \in A, \sigma(n) \in A$ then $A = \mathbb{N}$.

The axioms allow to define **addition** and **multiplication** in $\mathbb{N}$.

$\mathbb{Z}$ and $\mathbb{Q}$

The natural numbers allow **counting** but are not enough to solve even simpe equations as $aX + b = 0$, $a, b \in \mathbb{N}$

For, one introduces the **integers**

$$\mathbb{Z} = \frac{\mathbb{N} \times \mathbb{N}}{\sim}, \quad (m, n) \sim (m', n') \Leftrightarrow m + n' = n + m'.$$

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}, \quad m = \overline{(m, 0)}, -n = \overline{(0, n)},$$

and the **rational numbers**

$$\mathbb{Q} = \frac{\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})}{\sim} \quad (a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

$$\mathbb{Q} = \{0, \pm 1, \pm \frac{1}{2}, \pm 2, \pm \frac{1}{3}, ...\} \ni \frac{m}{n} = \overline{(m, n)}.$$

The natural numbers allow **counting** but are not enough to solve even simpe equations as $aX + b = 0$, $a, b \in \mathbb{N}$
For, one introduces the **integers**

$$\mathbb{Z} = \frac{\mathbb{N} \times \mathbb{N}}{\sim}, \quad (m, n) \sim (m', n') \Leftrightarrow m + n' = n + m'.$$

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}, \quad m = \overline{(m, 0)}, -n = \overline{(0, n)},$$

and the **rational numbers**

$$\mathbb{Q} = \frac{\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})}{\sim} \quad (a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

$$\mathbb{Q} = \{0, \pm 1, \pm \frac{1}{2}, \pm 2, \pm \frac{1}{3}, ...\} \ni \frac{m}{n} = \overline{(m, n)}.$$

$\mathbb{Z}$ and $\mathbb{Q}$

The natural numbers allow **counting** but are not enough to solve even simpe equations as $aX + b = 0$, $a, b \in \mathbb{N}$
For, one introduces the **integers**

$$\mathbb{Z} = \frac{\mathbb{N} \times \mathbb{N}}{\sim}, \quad (m, n) \sim (m', n') \Leftrightarrow m + n' = n + m'.$$

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}, \quad m = \overline{(m, 0)}, -n = \overline{(0, n)},$$

and the **rational numbers**

$$\mathbb{Q} = \frac{\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})}{\sim} \quad (a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

$$\mathbb{Q} = \{0, \pm 1, \pm\frac{1}{2}, \pm 2, \pm\frac{1}{3}, ...\} \ni \frac{m}{n} = \overline{(m, n)}.$$

Inadequacy of $\mathbb{Q}$

$\mathbb{Q}$ is the smallest **field** containing $\mathbb{N}$ and allows solutions of all equations

$$aX + b = 0, \quad a, b \in \mathbb{Q}$$

BUT

- More complicated algebraic equations cannot be solved in $\mathbb{Q}$.
- In particular, $\mathbb{Q}$ is not enough for **measuring**: Pythagoras (VI Century B.C.) already knew that the ratio between the lengths of the diagonal and the side of a square is not rational (i.e. $\sqrt{2} \notin \mathbb{Q}$)

These problems are (partially) solved with the introduction of the **real numbers** $\mathbb{R}$.

Inadequacy of $\mathbb{Q}$

$\mathbb{Q}$ is the smallest **field** containing $\mathbb{N}$ and allows solutions of all equations

$$aX + b = 0, \quad a, b \in \mathbb{Q}$$

BUT

- More complicated algebraic equations cannot be solved in $\mathbb{Q}$.
- In particular, $\mathbb{Q}$ is not enough for **measuring**: Pythagoras (VI Century B.C.) already knew that the ratio between the lengths of the diagonal and the side of a square is not rational (i.e. $\sqrt{2} \notin \mathbb{Q}$)

These problems are (partially) solved with the introduction of the **real numbers** $\mathbb{R}$.

One way to construct $\mathbb{R}$ is as follows:

$$\begin{aligned}\mathcal{C}(\mathbb{Q}) &= \{\text{Cauchy sequences in } \mathbb{Q}\}\\ &= \{(q_n)_{n\geq 0} \mid \forall \epsilon > 0, |q_m - q_n| < \epsilon \; \forall m, n \gg 0\}\end{aligned}$$

and then

$$\mathbb{R} = \frac{\mathcal{C}(\mathbb{Q})}{\sim} \quad \text{con } (q_n) \sim (q'_n) \Leftrightarrow \lim_{n\to\infty} |q_n - q'_n| = 0$$

Properties:

1. $\mathbb{Q} \hookrightarrow \mathbb{R}$, $q \mapsto \overline{(q_n = q)}$, with **dense** image.
2. $\mathbb{R}$ is a **complete** ordered field, meaning that every Cauchy sequence in $\mathbb{R}$ converges to an element in $\mathbb{R}$.
3. $\mathbb{R}$ is in bijection with the points of the euclidean line.

The real numbers

One way to construct $\mathbb{R}$ is as follows:

$$\begin{aligned} \mathcal{C}(\mathbb{Q}) &= \{\text{Cauchy sequences in } \mathbb{Q}\} \\ &= \{(q_n)_{n\geq 0} \mid \forall \epsilon > 0, |q_m - q_n| < \epsilon \ \forall m, n \gg 0\} \end{aligned}$$

and then

$$\mathbb{R} = \frac{\mathcal{C}(\mathbb{Q})}{\sim} \quad \text{con } (q_n) \sim (q_n') \Leftrightarrow \lim_{n\to\infty} |q_n - q_n'| = 0$$

Properties:

1. $\mathbb{Q} \hookrightarrow \mathbb{R}$, $q \mapsto \overline{(q_n = q)}$, with **dense** image.
2. $\mathbb{R}$ is a **complete** ordered field, meaning that every Cauchy sequence in $\mathbb{R}$ converges to an element in $\mathbb{R}$.
3. $\mathbb{R}$ is in bijection with the points of the euclidean line.

The real numbers

One way to construct $\mathbb{R}$ is as follows:

$$\begin{aligned}\mathcal{C}(\mathbb{Q}) &= \{\text{Cauchy sequences in } \mathbb{Q}\} \\ &= \{(q_n)_{n\geq 0} \mid \forall \epsilon > 0, |q_m - q_n| < \epsilon \ \forall m, n \gg 0\}\end{aligned}$$

and then

$$\mathbb{R} = \frac{\mathcal{C}(\mathbb{Q})}{\sim} \quad \text{con } (q_n) \sim (q'_n) \Leftrightarrow \lim_{n\to\infty} |q_n - q'_n| = 0$$

Properties:

1. $\mathbb{Q} \hookrightarrow \mathbb{R}$, $q \mapsto \overline{(q_n = q)}$, with **dense** image.
2. $\mathbb{R}$ is a **complete** ordered field, meaning that every Cauchy sequence in $\mathbb{R}$ converges to an element in $\mathbb{R}$.
3. $\mathbb{R}$ is in bijection with the points of the euclidean line.

Real numbers and equations

- the only irreducible polynomials in $\mathbb{R}[X]$ are $X^2 + aX + b$ with $a^2 - 4b < 0$.
- **Newton's method:** Let $f : \mathbb{R} \to \mathbb{R}$ be a differentiable function. Choose any $x_0 \in \mathbb{R}$ and define a sequence $\{x_n\}$ as

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

Under certain conditions, the sequence $\{x_n\}$ is Cauchy and if $\alpha = \lim_{n\to\infty} x_n$ then

$$f(\alpha) = 0.$$

Real numbers and equations

- the only irreducible polynomials in $\mathbb{R}[X]$ are $X^2 + aX + b$ with $a^2 - 4b < 0$.
- **Newton's method:** Let $f : \mathbb{R} \to \mathbb{R}$ be a differentiable function. Choose any $x_0 \in \mathbb{R}$ and define a sequence $\{x_n\}$ as

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

  Under certain conditions, the sequence $\{x_n\}$ is Cauchy and if $\alpha = \lim_{n\to\infty} x_n$ then

$$f(\alpha) = 0.$$

Analysis of the construction

Note that:

- The passage from $\mathbb{N}$ to $\mathbb{Z}$ and $\mathbb{Q}$ is straightforward, motivated by elementary algebraic considerations, and based on pure set-theoretic techniques.
- To construct $\mathbb{R}$ a new kind of structure had to be considered, namely a **metric** structure of $\mathbb{Q}$ (i.e. a **distance**).
- The distance in $\mathbb{Q}$ is defined by means of the absolute value: $d(q, q') = |q - q'|$.

So we may ask: are there other ways to endow $\mathbb{Q}$ with a distance? Or, are there other ways to define an absolute value in $\mathbb{Q}$?

It turns out that there are.

Analysis of the construction

Note that:

- The passage from $\mathbb{N}$ to $\mathbb{Z}$ and $\mathbb{Q}$ is straightforward, motivated by elementary algebraic considerations, and based on pure set-theoretic techniques.
- To construct $\mathbb{R}$ a new kind of structure had to be considered, namely a **metric** structure of $\mathbb{Q}$ (i.e. a **distance**).
- The distance in $\mathbb{Q}$ is defined by means of the absolute value: $d(q, q') = |q - q'|$.

So we may ask: are there other ways to endow $\mathbb{Q}$ with a distance? Or, are there other ways to define an absolute value in $\mathbb{Q}$?

It turns out that there are.

Analysis of the construction

Note that:

- The passage from $\mathbb{N}$ to $\mathbb{Z}$ and $\mathbb{Q}$ is straightforward, motivated by elementary algebraic considerations, and based on pure set-theoretic techniques.
- To construct $\mathbb{R}$ a new kind of structure had to be considered, namely a **metric** structure of $\mathbb{Q}$ (i.e. a **distance**).
- The distance in $\mathbb{Q}$ is defined by means of the absolute value: $d(q, q') = |q - q'|$.

So we may ask: are there other ways to endow $\mathbb{Q}$ with a distance? Or, are there other ways to define an absolute value in $\mathbb{Q}$?

It turns out that there are.

Analysis of the construction

Note that:

- The passage from $\mathbb{N}$ to $\mathbb{Z}$ and $\mathbb{Q}$ is straightforward, motivated by elementary algebraic considerations, and based on pure set-theoretic techniques.
- To construct $\mathbb{R}$ a new kind of structure had to be considered, namely a **metric** structure of $\mathbb{Q}$ (i.e. a **distance**).
- The distance in $\mathbb{Q}$ is defined by means of the absolute value: $d(q, q') = |q - q'|$.

So we may ask: are there other ways to endow $\mathbb{Q}$ with a distance? Or, are there other ways to define an absolute value in $\mathbb{Q}$?

It turns out that there are.

Analysis of the construction

Note that:

- The passage from $\mathbb{N}$ to $\mathbb{Z}$ and $\mathbb{Q}$ is straightforward, motivated by elementary algebraic considerations, and based on pure set-theoretic techniques.
- To construct $\mathbb{R}$ a new kind of structure had to be considered, namely a **metric** structure of $\mathbb{Q}$ (i.e. a **distance**).
- The distance in $\mathbb{Q}$ is defined by means of the absolute value: $d(q, q') = |q - q'|$.

So we may ask: are there other ways to endow $\mathbb{Q}$ with a distance? Or, are there other ways to define an absolute value in $\mathbb{Q}$?

It turns out that there are.

p-adic absolute value

$p \in \{2, 3, 5, 7, 11, 13, \dots\}$ a prime number. Given $\mathbb{Q} \ni q \neq 0$ write

$$q = p^r \frac{a}{b}, \quad \text{con } MCD(p, ab) = 1 \text{ e } r \in \mathbb{Z}.$$

Definition

*The p-**adic absolute value** of $q \in \mathbb{Q}$ is*

$$|q|_p = \begin{cases} p^{-r} & \textit{if } q \neq 0 \textit{ as above,} \\ 0 & \textit{se } q = 0. \end{cases}$$

NOTE: The powers p^n, $n > 0$, are "small": $|p^n|_p = \frac{1}{p^n} \to 0$.

From

1. $|q|_p = 0 \Leftrightarrow q = 0$,
2. $|qq'|_p = |q|_p|q'|_p$,
3. $|q + q'|_p \le \max(|q|_p, |q'|_p) \le |q|_p + |q'|_p$,

follows that

$$d_p : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}^{\ge 0} \quad d_p(x, y) = |x - y|_p$$

is a metric (p-**adic metric**).

Remark

p-adic metrics are all inequivalent to each other and the standard metric.

p-adic metric

From

1. $|q|_p = 0 \Leftrightarrow q = 0$,
2. $|qq'|_p = |q|_p|q'|_p$,
3. $|q+q'|_p \leq \max(|q|_p, |q'|_p) \leq |q|_p + |q'|_p$,

follows that

$$d_p : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}^{\geq 0} \quad d_p(x,y) = |x-y|_p$$

is a metric (p-**adic metric**).

Remark

p-adic metrics are all inequivalent to each other and the standard metric.

From

1. $|q|_p = 0 \Leftrightarrow q = 0$,
2. $|qq'|_p = |q|_p |q'|_p$,
3. $|q + q'|_p \leq \max(|q|_p, |q'|_p) \leq |q|_p + |q'|_p$,

follows that

$$d_p : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}^{\geq 0} \quad d_p(x, y) = |x - y|_p$$

is a metric (p-**adic metric**).

Remark

p-adic metrics are all inequivalent to each other and the standard metric.

Thus we can follow the same process used to construct $\mathbb{R}$:

1. Consider the set $\mathcal{C}_p(\mathbb{Q})$ of Cauchy sequences in $\mathbb{Q}$ for the p-adic metric.
2. Declare $(q_n) \sim (q'_n)$ iff $d_p(q_n, q'_n) \to 0$.
3. Define the **field of *p*-adic numbers** $\mathbb{Q}_p = \mathcal{C}_p(\mathbb{Q})/\sim$.

EXAMPLE: $(p = 5)$ Let $q_1 = 2$, $q_2 = 7$, $q_3 = 57$, $q_4 = 182$ and in general

$$q_{n+1} = q_n + k5^n, \quad \text{with } k \text{ s.t. } q_n^2 + 2kq_n5^n \equiv -1 \bmod 5^{n+1}.$$

We have

$$q_{n+k} - q_n \equiv 0 \bmod 5^n, \quad q_n^2 \equiv -1 \bmod 5^n$$

Thus (q_n) is Cauchy and if $\alpha = \lim_{n\to\infty} q_n$ then $\alpha^2 = -1$. I.e.

$$X^2 + 1 = 0 \text{ has solution in } \mathbb{Q}_5.$$

Thus we can follow the same process used to construct $\mathbb{R}$:

1. Consider the set $\mathcal{C}_p(\mathbb{Q})$ of Cauchy sequences in $\mathbb{Q}$ for the p-adic metric.
2. Declare $(q_n) \sim (q'_n)$ iff $d_p(q_n, q'_n) \to 0$.
3. Define the **field of p-adic numbers** $\mathbb{Q}_p = \mathcal{C}_p(\mathbb{Q})/\sim$.

EXAMPLE: $(p = 5)$ Let $q_1 = 2$, $q_2 = 7$, $q_3 = 57$, $q_4 = 182$ and in general

$$q_{n+1} = q_n + k5^n, \quad \text{with } k \text{ s.t. } q_n^2 + 2kq_n5^n \equiv -1 \bmod 5^{n+1}.$$

We have

$$q_{n+k} - q_n \equiv 0 \bmod 5^n, \quad q_n^2 \equiv -1 \bmod 5^n$$

Thus (q_n) is Cauchy and if $\alpha = \lim_{n\to\infty} q_n$ then $\alpha^2 = -1$. I.e.

$$X^2 + 1 = 0 \text{ has solution in } \mathbb{Q}_5.$$

Some properties of $\mathbb{Q}_p$

$\mathbb{Q}_p$ is very different from $\mathbb{R}$ in its basic structure:

- If $x \neq y \in \mathbb{Q}_p$, $d_p(x, y) \in p^{\mathbb{Z}}$. Thus, the spheres in $\mathbb{Q}_p$ are open and closed at the same time. Thus $\mathbb{Q}_p$ is **totally disconnected**.
- The **ultrametric inequality**

$$d_p(x, y) \leq \max\{d_p(x, z), d_p(y, z)\}$$

implies that

1. every point of a sphere can be taken as its center,
2. if two spheres have intersection, one is included in the other.
3. the closed sphere $\mathbb{Z}_p = \overline{S(0; 1)}$ is a **ring** which has as **unique maximal ideal** the sphere $S(0, 1) = p\mathbb{Z}_p$. Moreover

$$\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} \text{ and } \mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}].$$

Some properties of $\mathbb{Q}_p$

$\mathbb{Q}_p$ is very different from $\mathbb{R}$ in its basic structure:

- If $x \neq y \in \mathbb{Q}_p$, $d_p(x,y) \in p^{\mathbb{Z}}$. Thus, the spheres in $\mathbb{Q}_p$ are open and closed at the same time. Thus $\mathbb{Q}_p$ is **totally disconnected**.
- The **ultrametric inequality**

$$d_p(x,y) \leq \max\{d_p(x,z), d_p(y,z)\}$$

implies that

1. every point of a sphere can be taken as its center,
2. if two spheres have intersection, one is included in the other.
3. the closed sphere $\mathbb{Z}_p = \overline{S(0;1)}$ is a **ring** which has as **unique maximal ideal** the sphere $S(0,1) = p\mathbb{Z}_p$. Moreover

$$\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} \text{ and } \mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}].$$

The ring of p-**adic integers** $\mathbb{Z}_p$ can be described in terms of congruences as follows: Consider

$$\cdots \to \frac{\mathbb{Z}}{p^{n+1}\mathbb{Z}} \to \frac{\mathbb{Z}}{p^n\mathbb{Z}} \to \cdots \frac{\mathbb{Z}}{p^2\mathbb{Z}} \to \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

Let

$$\varprojlim \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right) = \left\{ (\bar{z}_n) \in \prod_{n\geq 1} \frac{\mathbb{Z}}{p^n\mathbb{Z}} \mid \bar{z}_{n+1} \mapsto \bar{z}_n \right\}$$

If $\{z_n\}$ is a sequence in $\mathbb{Z}$

$$\{z_n\} \text{ è di Cauchy} \Leftrightarrow \{\bar{z}_n\} \in \varprojlim(\mathbb{Z}/p^n\mathbb{Z}).$$

THUS: $\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z})$.

The ring of p-**adic integers** $\mathbb{Z}_p$ can be described in terms of congruences as follows: Consider

$$\cdots \to \frac{\mathbb{Z}}{p^{n+1}\mathbb{Z}} \to \frac{\mathbb{Z}}{p^n\mathbb{Z}} \to \cdots \frac{\mathbb{Z}}{p^2\mathbb{Z}} \to \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

Let

$$\varprojlim \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right) = \left\{ (\bar{z}_n) \in \prod_{n\geq 1} \frac{\mathbb{Z}}{p^n\mathbb{Z}} \mid \bar{z}_{n+1} \mapsto \bar{z}_n \right\}$$

If $\{z_n\}$ is a sequence in $\mathbb{Z}$

$$\{z_n\} \text{ è di Cauchy} \Leftrightarrow \{\bar{z}_n\} \in \varprojlim(\mathbb{Z}/p^n\mathbb{Z}).$$

THUS: $\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z}).$

p-adic expansions

Viewing $z \in \mathbb{Z}_p$ as an "organized set of congruence classes" yields the following explicit descriptions:

Let $\mathcal{A} = \{0, 1, \ldots, p-1\}$. Then

$$\mathbb{Z}_p = \left\{ \sum_{k=0}^{\infty} a_k p^k \mid a_k \in \mathcal{A} \right\},$$

$$\mathbb{Q}_p = \left\{ \sum_{k=-n}^{\infty} a_k p^k \mid a_k \in \mathcal{A} \right\},$$

This "expansion" of a p-adic number as a power series in p, should be seen as an analogue of the "expansion in base N" of a real number (with $\frac{1}{N}$ in place of p).

p-adic expansions

Viewing $z \in \mathbb{Z}_p$ as an "organized set of congruence classes" yields the following explicit descriptions:

Let $\mathcal{A} = \{0, 1, \ldots, p-1\}$. Then

$$\mathbb{Z}_p = \left\{ \sum_{k=0}^{\infty} a_k p^k \mid a_k \in \mathcal{A} \right\},$$

$$\mathbb{Q}_p = \left\{ \sum_{k=-n}^{\infty} a_k p^k \mid a_k \in \mathcal{A} \right\},$$

This "expansion" of a p-adic number as a power series in p, should be seen as an analogue of the "expansion in base N" of a real number (with $\frac{1}{N}$ in place of p).

p-adic expansions

Viewing $z \in \mathbb{Z}_p$ as an "organized set of congruence classes" yields the following explicit descriptions:

Let $\mathcal{A} = \{0, 1, \ldots, p-1\}$. Then

$$\mathbb{Z}_p = \left\{ \sum_{k=0}^{\infty} a_k p^k \mid a_k \in \mathcal{A} \right\},$$

$$\mathbb{Q}_p = \left\{ \sum_{k=-n}^{\infty} a_k p^k \mid a_k \in \mathcal{A} \right\},$$

This "expansion" of a p-adic number as a power series in p, should be seen as an analogue of the "expansion in base N" of a real number (with $\frac{1}{N}$ in place of p).

Hensel's Lemma

Equations in $\mathbb{Q}_p$ can be solved with an analogue of Newton's method:

Theorem (Hensel's Lemma)

Let $P(X) \in \mathbb{Z}_p[X]$ and suppose $x \in \mathbb{Z}_p$ is such that

$$|P(x)|_p < |P'(x)|_p^2.$$

Then there exists $\xi \in \mathbb{Z}_p$ with $d_p(\xi - x) < |P'(x)|_p$ such that $P(\xi) = 0$.

Proof (idea) : Let $x_1 = x - \frac{P(x)}{P'(x)}$. One sees that $d_p(x, x_1) < |P'(x)|_p$, $|P(x_1)|_p < |P(x)|_p$ and $|P'(x_1)|_p = |P'(x)|_p$. Iterate: $x_2 = x_1 - \frac{P(x_1)}{P'(x_1)}$ and so on. The sequence $x_1, x_2, x_3, \ldots$ is Cauchy and also $|P(x_{n+1})|_p < |P(x_n)|_p$. Thus $\xi = \lim x_n \in \mathbb{Z}_p$ and $P(\xi) = 0$.

Hensel's Lemma

Equations in $\mathbb{Q}_p$ can be solved with an analogue of Newton's method:

Theorem (Hensel's Lemma)

Let $P(X) \in \mathbb{Z}_p[X]$ and suppose $x \in \mathbb{Z}_p$ is such that

$$|P(x)|_p < |P'(x)|_p^2.$$

Then there exists $\xi \in \mathbb{Z}_p$ with $d_p(\xi - x) < |P'(x)|_p$ such that $P(\xi) = 0$.

Proof (idea) : Let $x_1 = x - \frac{P(x)}{P'(x)}$. One sees that $d_p(x, x_1) < |P'(x)|_p$, $|P(x_1)|_p < |P(x)|_p$ and $|P'(x_1)|_p = |P'(x)|_p$. Iterate: $x_2 = x_1 - \frac{P(x_1)}{P'(x_1)}$ and so on. The sequence $x_1, x_2, x_3, \ldots$ is Cauchy and also $|P(x_{n+1})|_p < |P(x_n)|_p$. Thus $\xi = \lim x_n \in \mathbb{Z}_p$ and $P(\xi) = 0$.

Hensel's Lemma

Equations in $\mathbb{Q}_p$ can be solved with an analogue of Newton's method:

Theorem (Hensel's Lemma)

Let $P(X) \in \mathbb{Z}_p[X]$ and suppose $x \in \mathbb{Z}_p$ is such that

$$|P(x)|_p < |P'(x)|_p^2.$$

Then there exists $\xi \in \mathbb{Z}_p$ with $d_p(\xi - x) < |P'(x)|_p$ such that $P(\xi) = 0$.

Proof (idea) : Let $x_1 = x - \frac{P(x)}{P'(x)}$. One sees that $d_p(x, x_1) < |P'(x)|_p$, $|P(x_1)|_p < |P(x)|_p$ and $|P'(x_1)|_p = |P'(x)|_p$. Iterate: $x_2 = x_1 - \frac{P(x_1)}{P'(x_1)}$ and so on. The sequence $x_1, x_2, x_3, \ldots$ is Cauchy and also $|P(x_{n+1})|_p < |P(x_n)|_p$. Thus $\xi = \lim x_n \in \mathbb{Z}_p$ and $P(\xi) = 0$.

Equations in $\mathbb{Q}_p$ can be solved with an analogue of Newton's method:

Theorem (Hensel's Lemma)

Let $P(X) \in \mathbb{Z}_p[X]$ and suppose $x \in \mathbb{Z}_p$ is such that

$$|P(x)|_p < |P'(x)|_p^2.$$

Then there exists $\xi \in \mathbb{Z}_p$ with $d_p(\xi - x) < |P'(x)|_p$ such that $P(\xi) = 0$.

Proof (idea) : Let $x_1 = x - \frac{P(x)}{P'(x)}$. One sees that $d_p(x, x_1) < |P'(x)|_p$, $|P(x_1)|_p < |P(x)|_p$ and $|P'(x_1)|_p = |P'(x)|_p$. Iterate: $x_2 = x_1 - \frac{P(x_1)}{P'(x_1)}$ and so on. The sequence $x_1, x_2, x_3, \ldots$ is Cauchy and also $|P(x_{n+1})|_p < |P(x_n)|_p$. Thus $\xi = \lim x_n \in \mathbb{Z}_p$ and $P(\xi) = 0$.

An application

Let $p > 2$, $n \in \mathbb{Z}$ not a square, but a square modulo p, i.e.

$$X^2 \equiv n \bmod p$$

has solution $X = a \in \mathbb{Z}$ (e.g. $3^2 = 9 \equiv 2 \bmod 7$).

Let $P(X) = X^2 - n \in \mathbb{Z}[X] \subset \mathbb{Z}_p[X]$. We have:

$$P(a) = a^2 - n \in \mathbb{Z}p \quad \Rightarrow \quad |P(a)|_p < 1$$
$$P'(a) = 2a \in \mathbb{Z} \setminus \mathbb{Z}p \quad \Rightarrow \quad |P'(a)|_p = 1$$

Hensel $\Longrightarrow$

$$\exists \xi \in \mathbb{Z}_p \text{ t.c. } \xi - a \in \mathbb{Z}_p p \text{ and } \xi^2 = n.$$

(in other words, $\sqrt{n} \in \mathbb{Z}_p$).

An application

Let $p > 2$, $n \in \mathbb{Z}$ not a square, but a square modulo p, i.e.

$$X^2 \equiv n \bmod p$$

has solution $X = a \in \mathbb{Z}$ (e.g. $3^2 = 9 \equiv 2 \bmod 7$).
Let $P(X) = X^2 - n \in \mathbb{Z}[X] \subset \mathbb{Z}_p[X]$. We have:

$$\begin{aligned} P(a) = a^2 - n \in \mathbb{Z}p \quad &\Rightarrow \quad |P(a)|_p < 1 \\ P'(a) = 2a \in \mathbb{Z} \setminus \mathbb{Z}p \quad &\Rightarrow \quad |P'(a)|_p = 1 \end{aligned}$$

Hensel $\Longrightarrow$

$$\exists \xi \in \mathbb{Z}_p \text{ t.c. } \xi - a \in \mathbb{Z}_p p \text{ and } \xi^2 = n.$$

(in other words, $\sqrt{n} \in \mathbb{Z}_p$).

An application

Let $p > 2$, $n \in \mathbb{Z}$ not a square, but a square modulo p, i.e.

$$X^2 \equiv n \bmod p$$

has solution $X = a \in \mathbb{Z}$ (e.g. $3^2 = 9 \equiv 2 \bmod 7$).
Let $P(X) = X^2 - n \in \mathbb{Z}[X] \subset \mathbb{Z}_p[X]$. We have:

$$\begin{aligned} P(a) = a^2 - n \in \mathbb{Z}p \quad &\Rightarrow \quad |P(a)|_p < 1 \\ P'(a) = 2a \in \mathbb{Z} \setminus \mathbb{Z}p \quad &\Rightarrow \quad |P'(a)|_p = 1 \end{aligned}$$

Hensel $\Longrightarrow$

$$\exists \xi \in \mathbb{Z}_p \text{ t.c. } \xi - a \in \mathbb{Z}_p p \text{ and } \xi^2 = n.$$

(in other words, $\sqrt{n} \in \mathbb{Z}_p$).

An application

Let $p > 2$, $n \in \mathbb{Z}$ not a square, but a square modulo p, i.e.

$$X^2 \equiv n \bmod p$$

has solution $X = a \in \mathbb{Z}$ (e.g. $3^2 = 9 \equiv 2 \bmod 7$).
Let $P(X) = X^2 - n \in \mathbb{Z}[X] \subset \mathbb{Z}_p[X]$. We have:

$$\begin{aligned} P(a) = a^2 - n \in \mathbb{Z}p \quad &\Rightarrow \quad |P(a)|_p < 1 \\ P'(a) = 2a \in \mathbb{Z} \setminus \mathbb{Z}p \quad &\Rightarrow \quad |P'(a)|_p = 1 \end{aligned}$$

Hensel $\Longrightarrow$

$$\exists \xi \in \mathbb{Z}_p \text{ t.c. } \xi - a \in \mathbb{Z}_p p \text{ and } \xi^2 = n.$$

(in other words, $\sqrt{n} \in \mathbb{Z}_p$).

A diagram

The situation is thus the following:

$$\begin{array}{ccc} a \in \mathbb{Z} & \hookrightarrow & \mathbb{Z}_p \ni \xi \\ \downarrow & \swarrow & \\ \mathbb{Z}/\mathbb{Z}p \ni \bar{a} = \bar{\xi} & & \end{array}$$

Thus, we can say that:

Remark

The construction of $\mathbb{Z}_p$ e $\mathbb{Q}_p$ provides a characteristic zero "environment" where to **"lift"** *solutions of equations in $\mathbb{Z}/\mathbb{Z}p$. This lift is meant in an algebraic sense: solutions in $\mathbb{Z}_p$ are* **inverse images** *of solutions in $\mathbb{Z}/\mathbb{Z}p$ under the* **quotient homomorphism**.

A diagram

The situation is thus the following:

$$\begin{array}{ccc} a \in \mathbb{Z} & \hookrightarrow & \mathbb{Z}_p \ni \xi \\ \downarrow & \swarrow & \\ \mathbb{Z}/\mathbb{Z}p \ni \bar{a} = \bar{\xi} & & \end{array}$$

Thus, we can say that:

Remark

The construction of $\mathbb{Z}_p$ e $\mathbb{Q}_p$ provides a characteristic zero "environment" where to **"lift"** *solutions of equations in $\mathbb{Z}/\mathbb{Z}p$. This lift is meant in an algebraic sense: solutions in $\mathbb{Z}_p$ are* **inverse images** *of solutions in $\mathbb{Z}/\mathbb{Z}p$ under the* **quotient homomorphism**.

More comparison between $\mathbb{R}$ and $\mathbb{Q}_p$

In $\mathbb{R}$ the equation $X^2 + 1$ has no solutions. The complex field $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ is algebraically closed and $[\mathbb{C} : \mathbb{R}] = 2$

Remark

There are no $\alpha \in \mathbb{Q}_p$ such that $\alpha^2 = p$.

Indeed: $\alpha^2 = p \Rightarrow |\alpha|_p^2 = \frac{1}{p} \Rightarrow |\alpha|_p = \frac{1}{\sqrt{p}}$. But the p-adic absolute value takes values integral powers of p on $\mathbb{Q}_p$.

In the same way we see that there is a proper chain of inclusions

$$\mathbb{Q}_p \subset \mathbb{Q}_p(p^{\frac{1}{2}}) \subset \mathbb{Q}_p(p^{\frac{1}{4}}) \subset \cdots \subset \mathbb{Q}_p(p^{\frac{1}{2n}}) \subset \cdots$$

In particular,

$$[\overline{\mathbb{Q}}_p : \mathbb{Q}_p] = \infty$$

More comparison between $\mathbb{R}$ and $\mathbb{Q}_p$

In $\mathbb{R}$ the equation $X^2 + 1$ has no solutions. The complex field $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ is algebraically closed and $[\mathbb{C} : \mathbb{R}] = 2$

Remark

There are no $\alpha \in \mathbb{Q}_p$ such that $\alpha^2 = p$.

Indeed: $\alpha^2 = p \Rightarrow |\alpha|_p^2 = \frac{1}{p} \Rightarrow |\alpha|_p = \frac{1}{\sqrt{p}}$. But the p-adic absolute value takes values integral powers of p on $\mathbb{Q}_p$.

In the same way we see that there is a proper chain of inclusions

$$\mathbb{Q}_p \subset \mathbb{Q}_p(p^{\frac{1}{2}}) \subset \mathbb{Q}_p(p^{\frac{1}{4}}) \subset \cdots \subset \mathbb{Q}_p(p^{\frac{1}{2n}}) \subset \cdots$$

In particular,

$$[\overline{\mathbb{Q}}_p : \mathbb{Q}_p] = \infty$$

More comparison between $\mathbb{R}$ and $\mathbb{Q}_p$

In $\mathbb{R}$ the equation $X^2 + 1$ has no solutions. The complex field $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ is algebraically closed and $[\mathbb{C} : \mathbb{R}] = 2$

Remark

There are no $\alpha \in \mathbb{Q}_p$ such that $\alpha^2 = p$.

Indeed: $\alpha^2 = p \Rightarrow |\alpha|_p^2 = \frac{1}{p} \Rightarrow |\alpha|_p = \frac{1}{\sqrt{p}}$. But the p-adic absolute value takes values integral powers of p on $\mathbb{Q}_p$.

In the same way we see that there is a proper chain of inclusions

$$\mathbb{Q}_p \subset \mathbb{Q}_p(p^{\frac{1}{2}}) \subset \mathbb{Q}_p(p^{\frac{1}{4}}) \subset \cdots \subset \mathbb{Q}_p(p^{\frac{1}{2n}}) \subset \cdots$$

In particular,

$$[\overline{\mathbb{Q}}_p : \mathbb{Q}_p] = \infty$$

A never ending game?

Theorem (Ostrowski)

A non-trivial absolute value $|\cdot|$ on $\mathbb{Q}$ is equivalent either to the standard absolute value $|\cdot|_\infty$ or to a p-adic absolute value $|\cdot|_p$.

Proof (idea) : Fix $\mathbb{Z} \ni a > 1$ and write every $b \in \mathbb{Z}$ in base a. If $b = c^n$ the triangle inequality yields

$$|c| \leq \max\{1, |a|^{\log c/\log a}\}.$$

1. $\exists c$ con $|c| > 1 \Rightarrow |a| > 1$. Then $|c|^{\frac{1}{\log c}} = |a|^{\frac{1}{\log a}}$ and $|\cdot| \sim |\cdot|_\infty$.
2. $\forall c \in \mathbb{Z}$, $|c| \leq 1 \Rightarrow J = \{a \in \mathbb{Z} \mid |a| < 1\}$ is a prime ideal in $\mathbb{Z}$. So $J = \mathbb{Z}p$ for a prime p and $|\cdot| \sim |\cdot|_p$.

A never ending game?

Theorem (Ostrowski)

A non-trivial absolute value $|\cdot|$ on $\mathbb{Q}$ is equivalent either to the standard absolute value $|\cdot|_\infty$ or to a p-adic absolute value $|\cdot|_p$.

Proof (idea) : Fix $\mathbb{Z} \ni a > 1$ and write every $b \in \mathbb{Z}$ in base a. If $b = c^n$ the triangle inequality yields

$$|c| \leq \max\{1, |a|^{\log c/\log a}\}.$$

1. $\exists c$ con $|c| > 1 \Rightarrow |a| > 1$. Then $|c|^{\frac{1}{\log c}} = |a|^{\frac{1}{\log a}}$ and $|\cdot| \sim |\cdot|_\infty$.
2. $\forall c \in \mathbb{Z}$, $|c| \leq 1 \Rightarrow J = \{a \in \mathbb{Z} \mid |a| < 1\}$ is a prime ideal in $\mathbb{Z}$. So $J = \mathbb{Z}p$ for a prime p and $|\cdot| \sim |\cdot|_p$.

A never ending game?

Theorem (Ostrowski)

A non-trivial absolute value $|\cdot|$ *on* $\mathbb{Q}$ *is equivalent either to the standard absolute value* $|\cdot|_\infty$ *or to a p-adic absolute value* $|\cdot|_p$.

Proof (idea) : Fix $\mathbb{Z} \ni a > 1$ and write every $b \in \mathbb{Z}$ in base a. If $b = c^n$ the triangle inequality yields

$$|c| \leq \max\{1, |a|^{\log c/\log a}\}.$$

1. $\exists c$ con $|c| > 1 \Rightarrow |a| > 1$. Then $|c|^{\frac{1}{\log c}} = |a|^{\frac{1}{\log a}}$ and $|\cdot| \sim |\cdot|_\infty$.
2. $\forall c \in \mathbb{Z}$, $|c| \leq 1 \Rightarrow J = \{a \in \mathbb{Z} \mid |a| < 1\}$ is a prime ideal in $\mathbb{Z}$. So $J = \mathbb{Z}p$ for a prime p and $|\cdot| \sim |\cdot|_p$.

A problem

Consider a non-degenerate quadratic form

$$Q(\vec{X}) = Q(X_1, \ldots, X_n) = \sum_{1 \le i \le j \le n} a_{ij} X_i X_j, \quad a_{ij} \in \mathbb{Q}$$

Problem

Find necessary and sufficient conditions for the existence of $\mathbb{Q}^n \ni \vec{q} \neq (0, \ldots, 0)$ *with* $Q(\vec{q}) = 0$.

NOTE: The equation

$$X^2 - 2Y^2 = 0$$

has real non-zero solutions (e.g. $(\sqrt{2}, 1)$) but no rational solutions (because $\sqrt{2} \notin \mathbb{Q}$). Thus the existence of real solutions is a **necessary, but not sufficient** condition for the existence of rational solutions.

A problem

Consider a non-degenerate quadratic form

$$Q(\vec{X}) = Q(X_1, \dots, X_n) = \sum_{1 \le i \le j \le n} a_{ij} X_i X_j, \quad a_{ij} \in \mathbb{Q}$$

Problem

Find necessary and sufficient conditions for the existence of $\mathbb{Q}^n \ni \vec{q} \neq (0, \dots, 0)$ *with* $Q(\vec{q}) = 0$.

NOTE: The equation

$$X^2 - 2Y^2 = 0$$

has real non-zero solutions (e.g. $(\sqrt{2}, 1)$) but no rational solutions (because $\sqrt{2} \notin \mathbb{Q}$). Thus the existence of real solutions is a **necessary, but not sufficient** condition for the existence of rational solutions.

A problem

Consider a non-degenerate quadratic form

$$Q(\vec{X}) = Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j, \quad a_{ij} \in \mathbb{Q}$$

Problem

Find necessary and sufficient conditions for the existence of $\mathbb{Q}^n \ni \vec{q} \neq (0, \ldots, 0)$ *with* $Q(\vec{q}) = 0$.

NOTE: The equation

$$X^2 - 2Y^2 = 0$$

has real non-zero solutions (e.g. $(\sqrt{2}, 1)$) but no rational solutions (because $\sqrt{2} \notin \mathbb{Q}$). Thus the existence of real solutions is a **necessary, but not sufficient** condition for the existence of rational solutions.

Every solution in $\mathbb{Q}^n$ of an equation

$$F(X_1, \ldots, X_n) = 0$$

is also a solution in $\mathbb{R}^n$ and $\mathbb{Q}_p^n$ for all p.

Theorem (Hasse principle)

Let $Q(\vec{X}) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j$, with $a_{ij} \in \mathbb{Q}$. The equation $Q(\vec{X}) = 0$ admits a non-zero solution in $\mathbb{Q}^n$ if and only if it admits non-zero solutions in $\mathbb{R}^n$ and in $\mathbb{Q}_p^n$ for every p.

Proof: The proof is not constructive and not easy. See Part I of Serre's *Cours d'arithmetique*.

Hasse principle

Every solution in $\mathbb{Q}^n$ of an equation

$$F(X_1, \ldots, X_n) = 0$$

is also a solution in $\mathbb{R}^n$ and $\mathbb{Q}_p^n$ for all p.

Theorem (Hasse principle)

Let $Q(\vec{X}) = \sum_{1 \le i \le j \le n} a_{ij} X_i X_j$, with $a_{ij} \in \mathbb{Q}$. The equation $Q(\vec{X}) = 0$ admits a non-zero solution in $\mathbb{Q}^n$ if and only if it admits non-zero solutions in $\mathbb{R}^n$ and in $\mathbb{Q}_p^n$ for every p.

Proof: The proof is not constructive and not easy. See Part I of Serre's *Cours d'arithmetique*.

Hasse principle

Every solution in $\mathbb{Q}^n$ of an equation

$$F(X_1, \ldots, X_n) = 0$$

is also a solution in $\mathbb{R}^n$ and $\mathbb{Q}_p^n$ for all p.

Theorem (Hasse principle)

Let $Q(\vec{X}) = \sum_{1 \le i \le j \le n} a_{ij} X_i X_j$, with $a_{ij} \in \mathbb{Q}$. The equation $Q(\vec{X}) = 0$ admits a non-zero solution in $\mathbb{Q}^n$ if and only if it admits non-zero solutions in $\mathbb{R}^n$ and in $\mathbb{Q}_p^n$ for every p.

Proof: The proof is not constructive and not easy. See Part I of Serre's *Cours d'arithmetique*.

Quaternion algebras

A **quaternion algebra** over a field K is an algebra of the form

$$D = K \oplus Ki \oplus Kj \oplus Kij \quad ji = -ij, i^2 = a, j^2 = b, \quad a, b \in K^\times$$

e.g. the **Hamilton quaternions** ($K = \mathbb{R}$, $a = b = -1$)

Theorem

If $K = \mathbb{R}$ or $\mathbb{Q}_p$ there are only two quaternion algebras up to isomorphism:

1. $D \simeq M_2(K)$ $(a = b = 1)$,
2. $D \simeq$ *the unique central division algebra over K of rank 4.*

Quaternion algebras

A **quaternion algebra** over a field K is an algebra of the form

$$D = K \oplus Ki \oplus Kj \oplus Kij \quad ji = -ij, i^2 = a, j^2 = b, \quad a, b \in K^\times$$

e.g. the **Hamilton quaternions** ($K = \mathbb{R}$, $a = b = -1$)

Theorem

If $K = \mathbb{R}$ or $\mathbb{Q}_p$ there are only two quaternion algebras up to isomorphism:

1. $D \simeq M_2(K)$ $(a = b = 1)$,
2. $D \simeq$ *the unique central division algebra over K of rank 4.*

Quaternion algebras over $\mathbb{Q}$

What about quaternion algebras over $\mathbb{Q}$?

Given D over $\mathbb{Q}$, let $D \otimes \mathbb{Q}_p$ the algebras over $\mathbb{Q}_p$ with the same constants a, b. (**Notation:** $\mathbb{Q}_\infty = \mathbb{R}$)

Theorem

Let $\Sigma(D) \subset \{\infty, 2, 3, 5, \ldots\}$ be the set of primes such that $D \otimes \mathbb{Q}_p$ is a division algebra. Then:

1. $\Sigma(M_2(\mathbb{Q})) = \emptyset$.
2. $\Sigma(D)$ *is a finite set consisting of an even number of elements.*
3. $D \simeq D'$ *iff* $\Sigma(D) = \Sigma(D')$.
4. *If* Σ *is finite and even there is one quaternion algebra* D *over* $\mathbb{Q}$ *such that* $\Sigma(D) = \Sigma$

Quaternion algebras over $\mathbb{Q}$

What about quaternion algebras over $\mathbb{Q}$?

Given D over $\mathbb{Q}$, let $D \otimes \mathbb{Q}_p$ the algebras over $\mathbb{Q}_p$ with the same constants a, b. (**Notation:** $\mathbb{Q}_\infty = \mathbb{R}$)

Theorem

Let $\Sigma(D) \subset \{\infty, 2, 3, 5, \ldots\}$ be the set of primes such that $D \otimes \mathbb{Q}_p$ is a division algebra. Then:

1. $\Sigma(M_2(\mathbb{Q})) = \emptyset$.
2. $\Sigma(D)$ *is a finite set consisting of an even number of elements.*
3. $D \simeq D'$ *iff* $\Sigma(D) = \Sigma(D')$.
4. *If* Σ *is finite and even there is one quaternion algebra* D *over* $\mathbb{Q}$ *such that* $\Sigma(D) = \Sigma$

Quaternion algebras over $\mathbb{Q}$

What about quaternion algebras over $\mathbb{Q}$?

Given D over $\mathbb{Q}$, let $D \otimes \mathbb{Q}_p$ the algebras over $\mathbb{Q}_p$ with the same constants a, b. (**Notation:** $\mathbb{Q}_\infty = \mathbb{R}$)

Theorem

Let $\Sigma(D) \subset \{\infty, 2, 3, 5, ...\}$ be the set of primes such that $D \otimes \mathbb{Q}_p$ is a division algebra. Then:

1. $\Sigma(M_2(\mathbb{Q})) = \emptyset$.
2. $\Sigma(D)$ *is a finite set consisting of an even number of elements.*
3. $D \simeq D'$ *iff* $\Sigma(D) = \Sigma(D')$.
4. *If* Σ *is finite and even there is one quaternion algebra* D *over* $\mathbb{Q}$ *such that* $\Sigma(D) = \Sigma$

Some textbooks:

1. A. M. Robert, *A Course in p-adic Analysis*, Springer GTM 198
2. A. Frölich, *Local Fields*, in Algebraic Number Theory, Academic Press (1967)
3. J. W. S. Cassels, *Global Fields*, in Algebraic Number Theory, Academic Press (1967)
4. J.-P. Serre, *A Course in Arithmetic*. Springer GTM 7
5. M.F. Vigneras, *Arithmtique des Algbres de Quaternions*, LNM 800, Springer (1980)

$\mathbb{E}\ \mathbb{N}\ \mathbb{D}$