The Importance of Being Totally Disconnected

Giancarlo Castellano

10th April, 2019

About the title. . .

- "Totally disconnected" is a notion from point-set topology.

About the title...

- "Totally disconnected" is a notion from point-set topology.
- Recall that a topological space is *connected* if it cannot be written as a disjoint union of non-empty open subsets, and *disconnected* otherwise.

About the title...

- "Totally disconnected" is a notion from point-set topology.
- Recall that a topological space is *connected* if it cannot be written as a disjoint union of non-empty open subsets, and *disconnected* otherwise.

Examples

- $\mathbb{R}$ is connected.

About the title...

- "Totally disconnected" is a notion from point-set topology.
- Recall that a topological space is *connected* if it cannot be written as a disjoint union of non-empty open subsets, and *disconnected* otherwise.

Examples

- $\mathbb{R}$ is connected.
- $\mathbb{Q}$ is disconnected.

About the title...

- "Totally disconnected" is a notion from point-set topology.
- Recall that a topological space is *connected* if it cannot be written as a disjoint union of non-empty open subsets, and *disconnected* otherwise.
- A space is disconnected iff it has some proper subset which is both open and closed ($=:$ *clopen*).

Examples

- $\mathbb{R}$ is connected.
- $\mathbb{Q}$ is disconnected.

About the title...

- "Totally disconnected" is a notion from point-set topology.
- Recall that a topological space is *connected* if it cannot be written as a disjoint union of non-empty open subsets, and *disconnected* otherwise.
- A space is disconnected iff it has some proper subset which is both open and closed ($=:$ *clopen*).

Examples

- $\mathbb{R}$ is connected.
- $\mathbb{Q}$ is disconnected.

- A space is *totally disconnected* if around each point one can find arbitrarily small clopen sets.

About the title. . . , II

- The title is inspired by *The Importance of Being Ernest*, a play by Oscar Wilde.

About the title. . . , II

- The title is inspired by *The Importance of Being Ernest*, a play by Oscar Wilde.
- The play is about how it is important to be *earnest* (= serious), but the play itself is not at all serious.

About the title. . . , II

- The title is inspired by *The Importance of Being Ernest*, a play by Oscar Wilde.
- The play is about how it is important to be *earnest* (= serious), but the play itself is not at all serious.
- Similarly, this talk is not very serious.

About the title. . . , II

- The title is inspired by *The Importance of Being Ernest*, a play by Oscar Wilde.
- The play is about how it is important to be *earnest* (= serious), but the play itself is not at all serious.
- Similarly, this talk is not very serious. But hopefully it is not *totally* disconnected.

I remember vividly. . .

I remember vividly. . .

. . . my geometry homework from middle school on the Pythagorean theorem.

I remember vividly. . .

. . . my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;

I remember vividly. . .

. . . my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;

I remember vividly. . .

. . . my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;
- $(7, 24, 25)$;

I remember vividly. . .

. . . my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;
- $(7, 24, 25)$;
- $(9, 40, 41)$;

I remember vividly...

...my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;
- $(7, 24, 25)$;
- $(9, 40, 41)$;
- $\left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right)$ for q odd;

I remember vividly...

...my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;
- $(7, 24, 25)$;
- $(9, 40, 41)$;
- $\left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right)$ for q odd;
- $(8, 15, 17)$.

I remember vividly...

...my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;
- $(7, 24, 25)$;
- $(9, 40, 41)$;
- $\left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right)$ for q odd;
- $(8, 15, 17)$.

Do not restrict to integers:

$(8, 15, 17)$

I remember vividly...

...my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;
- $(7, 24, 25)$;
- $(9, 40, 41)$;
- $\left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right)$ for q odd;
- $(8, 15, 17)$.

Do not restrict to integers:

$(8, 15, 17) \rightsquigarrow \left(4, \frac{15}{2}, \frac{17}{2}\right)$

I remember vividly...

... my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;
- $(7, 24, 25)$;
- $(9, 40, 41)$;
- $\left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right)$ for q odd;
- $(8, 15, 17)$.

Do not restrict to integers:

$$(8, 15, 17) \rightsquigarrow \left(4, \frac{15}{2}, \frac{17}{2}\right) = \left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right) \text{ with } q = 4.$$

I remember vividly. . .

. . . my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;
- $(7, 24, 25)$;
- $(9, 40, 41)$;
- $\left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right)$ for q odd;
- $(8, 15, 17)$.

Do not restrict to integers:

$$(8, 15, 17) \rightsquigarrow \left(4, \tfrac{15}{2}, \tfrac{17}{2}\right) = \left(q, \tfrac{q^2-1}{2}, \tfrac{q^2+1}{2}\right) \text{ with } q = 4.$$

Thus, every triple (a, b, c) of rational numbers with $a^2 + b^2 = c^2$ is of the above form up to scaling.

I remember vividly...

...my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;
- $(7, 24, 25)$;
- $(9, 40, 41)$;
- $\left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right)$ for q odd;
- $(8, 15, 17)$.

Do not restrict to integers:

$$(8, 15, 17) \rightsquigarrow \left(4, \frac{15}{2}, \frac{17}{2}\right) = \left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right) \text{ with } q = 4.$$

Thus, every triple (a, b, c) of rational numbers with $a^2 + b^2 = c^2$ is of the above form up to scaling.

$\rightsquigarrow$ classification of integer solutions.

I remember vividly...

... my geometry homework from middle school on the Pythagorean theorem.

Examples

Commonly encountered Pythagorean triples:

- $(3, 4, 5)$;
- $(5, 12, 13)$;
- $(7, 24, 25)$;
- $(9, 40, 41)$;
- $\left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right)$ for q odd;
- $(8, 15, 17)$.

Do not restrict to integers:

$$(8, 15, 17) \rightsquigarrow \left(4, \frac{15}{2}, \frac{17}{2}\right) = \left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right) \text{ with } q = 4.$$

Thus, every triple (a, b, c) of rational numbers with $a^2 + b^2 = c^2$ is of the above form up to scaling.

$\rightsquigarrow$ classification of integer solutions. $\rightsquigarrow$ classification of Pythagorean triples.

After all this time...

Back then	Now

After all this time...

Back then	Now
Solutions over $\mathbb{Z}$	

After all this time...

Back then	Now
Solutions over $\mathbb{Z}$	Solutions over $\mathbb{Q}$ (nicer theory)

After all this time...

Back then	Now
Solutions over $\mathbb{Z}$	Solutions over $\mathbb{Q}$ (nicer theory)
Easy concrete example: $x^2 + y^2 = z^2$	

After all this time...

Back then	Now
Solutions over $\mathbb{Z}$	Solutions over $\mathbb{Q}$ (nicer theory)
Easy concrete example: $x^2 + y^2 = z^2$	General question: $p(x_1, \ldots, x_n) = 0$ quadratic equation with coefficients in $\mathbb{Z}$

After all this time...

Back then	Now
Solutions over $\mathbb{Z}$	Solutions over $\mathbb{Q}$ (nicer theory)
Easy concrete example: $x^2 + y^2 = z^2$	General question: $p(x_1, \ldots, x_n) = 0$ quadratic equation with coefficients in $\mathbb{Z}$
Child who should watch more TV	

After all this time...

Back then	Now
Solutions over $\mathbb{Z}$	Solutions over $\mathbb{Q}$ (nicer theory)
Easy concrete example: $x^2 + y^2 = z^2$	General question: $p(x_1, \ldots, x_n) = 0$ quadratic equation with coefficients in $\mathbb{Z}$
Child who should watch more TV	PhD student who should watch less TV

After all this time...

Back then	Now
Solutions over $\mathbb{Z}$	Solutions over $\mathbb{Q}$ (nicer theory)
Easy concrete example: $x^2 + y^2 = z^2$	General question: $p(x_1, \ldots, x_n) = 0$ quadratic equation with coefficients in $\mathbb{Z}$
Child who should watch more TV	PhD student who should watch less TV
	Finding *real* solutions is much easier

After all this time...

Back then	Now
Solutions over $\mathbb{Z}$	Solutions over $\mathbb{Q}$ (nicer theory)
Easy concrete example: $x^2 + y^2 = z^2$	General question: $p(x_1, \ldots, x_n) = 0$ quadratic equation with coefficients in $\mathbb{Z}$
Child who should watch more TV	PhD student who should watch less TV
No idea what a real number is	Finding *real* solutions is much easier

$\mathbb{R}$eally easy

Task

Find solutions of

$$x^2 + y^2 = z^2.$$

over $\mathbb{R}$.

$\mathbb{R}$eally easy

Task

Find solutions of

$$x^2 + y^2 = z^2.$$

over $\mathbb{R}$.

Solution

Pick any $x, y \in \mathbb{R}$, then

$$x^2 + y^2 = z^2$$

$\mathbb{R}$eally easy

Task

Find solutions of

$$x^2 + y^2 = z^2.$$

over $\mathbb{R}$.

Solution

Pick any $x, y \in \mathbb{R}$, then

$$0 \leq x^2 + y^2 = z^2$$

$\mathbb{R}$eally easy

Task

Find solutions of

$$x^2 + y^2 = z^2.$$

over $\mathbb{R}$.

Solution

Pick any $x, y \in \mathbb{R}$, then

$$0 \leq x^2 + y^2 = z^2$$

always has a solution $\left(x, y, \sqrt{x^2 + y^2}\right)$.

$\mathbb{R}$eally easy

Task

Find solutions of

$$x^2 + y^2 = z^2.$$

over $\mathbb{R}$.

Solution

Pick any $x, y \in \mathbb{R}$, then

$$0 \leq x^2 + y^2 = z^2$$

always has a solution $\left(x, y, \sqrt{x^2 + y^2}\right)$. This is because

$$x \text{ is a square in } \mathbb{R} \iff x \geq 0.$$

$\mathbb{Q}$uite hard

$\mathbb{Q}$uite hard

$$x \text{ is a square in } \mathbb{Q} \implies x \geq 0$$

$$\text{but not } \impliedby$$

$\mathbb{Q}$uite hard

$$x \text{ is a square in } \mathbb{Q} \implies x \geq 0$$
$$\text{but not} \quad \Longleftarrow$$

Theorem (Fundamental Theorem of Arithmetic)

Let m be a nonzero integer. Then

$$m = \pm \prod_p p^{v_p}$$

for unique natural numbers $v_p = v_p(m)$. (The product is finite.)

$\mathbb{Q}$uite hard

$$x \text{ is a square in } \mathbb{Q} \implies x \geq 0$$
$$\text{but not} \quad \impliedby$$

Theorem (Fundamental Theorem of Arithmetic)

Let x be a nonzero rational number. Then

$$x = \pm \prod_p p^{v_p}$$

for unique integers $v_p = v_p(x)$. (The product is finite.)

$\mathbb{Q}$uite hard

$$x \text{ is a square in } \mathbb{Q} \implies x \geq 0$$

$$\text{but not } \impliedby$$

Theorem (Fundamental Theorem of Arithmetic)

Let x be a nonzero rational number. Then

$$x = \pm \prod_p p^{v_p}$$

for unique integers $v_p = v_p(x)$. (The product is finite.)

Corollary

Let x be a nonzero rational number. Then x is a square if and only if $x > 0$ and $v_p(x)$ is even for all p.

Order!

- v_p can be interpreted as the *order* of vanishing / of a pole (cf. meromorphic functions).

Order!

- v_p can be interpreted as the *order* of vanishing / of a pole (cf. meromorphic functions).
- More precisely, every nonzero rational number x can be written as a "Laurent series"

Order!

- v_p can be interpreted as the *order* of vanishing / of a pole (cf. meromorphic functions).

- More precisely, every nonzero rational number x can be written as a "Laurent series"

$$x = \sum_{i=\nu}^{\infty} a_i p^i, \qquad \nu \in \mathbb{Z}, a_i \in \{0, \dots, p-1\},$$

where the index ν of the leading term is precisely $v_p(x)$.

Order!

- v_p can be interpreted as the *order* of vanishing / of a pole (cf. meromorphic functions).

- More precisely, every nonzero rational number x can be written as a "Laurent series"

$$x = \sum_{i=\nu}^{\infty} a_i p^i, \qquad \nu \in \mathbb{Z}, a_i \in \{0, \ldots, p-1\},$$

where the index ν of the leading term is precisely $v_p(x)$.

- Indeed, if $x = m$ is a positive integer, $\nu = v_p(m)$, then

$$m = a_\nu p^\nu + a_{\nu+1} p^{\nu+1} + \cdots + a_{d-1} p^{d-1} + a_d p^d \qquad \text{(finite sum)}$$

with $a_i \in \{0, \ldots, p-1\}$ for all i. (Base-p representation.)

Order!, cont'd

- We can then write $x = \frac{1}{m}$ as a Laurent series $\sum_{i=\ell}^{\infty} b_i p^i$ by comparing coefficients of p^i in the equality

$$(a_\nu p^\nu + \cdots + a_d p^d) \cdot (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 1$$

Order!, cont'd

- We can then write $x = \frac{1}{m}$ as a Laurent series $\sum_{i=\ell}^{\infty} b_i p^i$ by comparing coefficients of p^i in the equality

$$(a_\nu p^\nu + \cdots + a_d p^d) \cdot (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 1$$

Note that the order ℓ of this series is $\ell = -\nu$

Order!, cont'd

- We can then write $x = \frac{1}{m}$ as a Laurent series $\sum_{i=\ell}^{\infty} b_i p^i$ by comparing coefficients of p^i in the equality

$$(a_\nu p^\nu + \cdots + a_d p^d) \cdot (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 1$$

Note that the order ℓ of this series is $\ell = -\nu = -v_p(m)$

Order!, cont'd

- We can then write $x = \frac{1}{m}$ as a Laurent series $\sum_{i=\ell}^{\infty} b_i p^i$ by comparing coefficients of p^i in the equality

$$(a_\nu p^\nu + \cdots + a_d p^d) \cdot (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 1$$

  Note that the order ℓ of this series is $\ell = -\nu = -v_p(m)$ $= v_p(x)$.

Order!, cont'd

- We can then write $x = \frac{1}{m}$ as a Laurent series $\sum_{i=\ell}^{\infty} b_i p^i$ by comparing coefficients of p^i in the equality

$$(a_\nu p^\nu + \cdots + a_d p^d) \cdot (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 1$$

  Note that the order ℓ of this series is $\ell = -\nu = -v_p(m)$ $= v_p(x)$.

- Similarly, for given $x = \sum_{i=\nu}^{\infty} a_i p^i$, the expansion of $-x$ is given by solving for b_i in the equality

$$(a_\nu p^\nu + a_{\nu+1} p^{\nu+1} + \cdots) + (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 0.$$

Order!, cont'd

- We can then write $x = \frac{1}{m}$ as a Laurent series $\sum_{i=\ell}^{\infty} b_i p^i$ by comparing coefficients of p^i in the equality

$$(a_\nu p^\nu + \cdots + a_d p^d) \cdot (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 1$$

  Note that the order ℓ of this series is $\ell = -\nu = -v_p(m)$ $= v_p(x)$.

- Similarly, for given $x = \sum_{i=\nu}^{\infty} a_i p^i$, the expansion of $-x$ is given by solving for b_i in the equality

$$(a_\nu p^\nu + a_{\nu+1} p^{\nu+1} + \cdots) + (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 0.$$

  Here $\ell = \nu = v_p(x) = v_p(-x)$.

Order!, cont'd

- We can then write $x = \frac{1}{m}$ as a Laurent series $\sum_{i=\ell}^{\infty} b_i p^i$ by comparing coefficients of p^i in the equality

$$(a_\nu p^\nu + \cdots + a_d p^d) \cdot (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 1$$

Note that the order ℓ of this series is $\ell = -\nu = -v_p(m)$ $= v_p(x)$.

- Similarly, for given $x = \sum_{i=\nu}^{\infty} a_i p^i$, the expansion of $-x$ is given by solving for b_i in the equality

$$(a_\nu p^\nu + a_{\nu+1} p^{\nu+1} + \cdots) + (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 0.$$

Here $\ell = \nu = v_p(x) = v_p(-x)$.

Examples

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$$

Order!, cont'd

- We can then write $x = \frac{1}{m}$ as a Laurent series $\sum_{i=\ell}^{\infty} b_i p^i$ by comparing coefficients of p^i in the equality

$$(a_\nu p^\nu + \cdots + a_d p^d) \cdot (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 1$$

Note that the order ℓ of this series is $\ell = -\nu = -v_p(m)$ $= v_p(x)$.

- Similarly, for given $x = \sum_{i=\nu}^{\infty} a_i p^i$, the expansion of $-x$ is given by solving for b_i in the equality

$$(a_\nu p^\nu + a_{\nu+1} p^{\nu+1} + \cdots) + (b_\ell p^\ell + b_{\ell+1} p^{\ell+1} + \cdots) = 0.$$

Here $\ell = \nu = v_p(x) = v_p(-x)$.

Examples

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots = (p-1) \cdot \frac{1}{1-p}.$$

$\mathbb{R}$emember...

In summary, we have proved:

$\mathbb{R}$emember...

In summary, we have proved:

Lemma

Let p a prime. Then every rational number can be written as a "Laurent series"

$$\sum_{i=\nu}^{\infty} a_i p^i, \qquad \nu \in \mathbb{Z}, a_i \in \{0, \ldots, p-1\} \tag{*}$$

where the expansion is either finite or periodic.

ℝemember...

In summary, we have proved:

Lemma

Let p a prime. Then every rational number can be written as a "Laurent series"

$$\sum_{i=\nu}^{\infty} a_i p^i, \qquad \nu \in \mathbb{Z}, a_i \in \{0, \ldots, p-1\} \tag{*}$$

where the expansion is either finite or periodic.

(Cf.: Every rational number can be written as $\sum_{i=\nu}^{\infty} c_i \varepsilon^i$ with, say, $\varepsilon = 1/10$, $c_i \in \{0, \ldots, 9\}$, with expansion either finite or periodic.

$\mathbb{R}$emember...

In summary, we have proved:

Lemma

Let p a prime. Then every rational number can be written as a "Laurent series"

$$\sum_{i=\nu}^{\infty} a_i p^i, \qquad \nu \in \mathbb{Z}, a_i \in \{0, \ldots, p-1\} \tag{*}$$

where the expansion is either finite or periodic.

(Cf.: Every rational number can be written as $\sum_{i=\nu}^{\infty} c_i \varepsilon^i$ with, say, $\varepsilon = 1/10$, $c_i \in \{0, \ldots, 9\}$, with expansion either finite or periodic. Allowing for arbitrary expansions yields the reals.)

$\mathbb{R}$emember...

In summary, we have proved:

Lemma

Let p a prime. Then every rational number can be written as a "Laurent series"

$$\sum_{i=\nu}^{\infty} a_i p^i, \qquad \nu \in \mathbb{Z}, a_i \in \{0, \ldots, p-1\} \tag{*}$$

where the expansion is either finite or periodic.

(Cf.: Every rational number can be written as $\sum_{i=\nu}^{\infty} c_i \varepsilon^i$ with, say, $\varepsilon = 1/10$, $c_i \in \{0, \ldots, 9\}$, with expansion either finite or periodic. Allowing for arbitrary expansions yields the reals.)

Definition

Let p be a prime. Then the expressions of the form (*) form the *field of p-adic numbers*, denoted $\mathbb{Q}_p$.

Let's recap

We just defined a field $\mathbb{Q}_p$ for each prime p, whose elements look like "Laurent series" in the "variable" p.

Let's recap

We just defined a field $\mathbb{Q}_p$ for each prime p, whose elements look like "Laurent series" in the "variable" p.

We were trying to find a correct interpretation of the exponents v_p.

Let's recap

We just defined a field $\mathbb{Q}_p$ for each prime p, whose elements look like "Laurent series" in the "variable" p.

We were trying to find a correct interpretation of the exponents v_p.

Definition

For x in $\mathbb{Q}_p$, $x \neq 0$,

$$v_p(x) := \text{ smallest index in the } p\text{-adic expansion of } x.$$

Let's recap

We just defined a field $\mathbb{Q}_p$ for each prime p, whose elements look like "Laurent series" in the "variable" p.

We were trying to find a correct interpretation of the exponents v_p.

Definition

For x in $\mathbb{Q}_p$, $x \neq 0$,

$$v_p(x) := \text{ smallest index in the } p\text{-adic expansion of } x.$$

Observe: If x in $\mathbb{Q}_p$ is a nonzero square, then $v_p(x)$ is even.

Let's recap

We just defined a field $\mathbb{Q}_p$ for each prime p, whose elements look like "Laurent series" in the "variable" p.

We were trying to find a correct interpretation of the exponents v_p.

Definition

For x in $\mathbb{Q}_p$, $x \neq 0$,

$$v_p(x) := \text{ smallest index in the } p\text{-adic expansion of } x.$$

Observe: If x in $\mathbb{Q}_p$ is a nonzero square, then $v_p(x)$ is even.So our previous corollary becomes:

Let's recap

We just defined a field $\mathbb{Q}_p$ for each prime p, whose elements look like "Laurent series" in the "variable" p.

We were trying to find a correct interpretation of the exponents v_p.

Definition

For x in $\mathbb{Q}_p$, $x \neq 0$,

$$v_p(x) := \text{ smallest index in the } p\text{-adic expansion of } x.$$

Observe: If x in $\mathbb{Q}_p$ is a nonzero square, then $v_p(x)$ is even.So our previous corollary becomes:

Proposition

A nonzero rational number $x \in \mathbb{Q}$ is a square if and only if it is a square in $\mathbb{R}$ and in each $\mathbb{Q}_p$.

Let's recap

We just defined a field $\mathbb{Q}_p$ for each prime p, whose elements look like "Laurent series" in the "variable" p.

We were trying to find a correct interpretation of the exponents v_p.

Definition

For x in $\mathbb{Q}_p$, $x \neq 0$,

$$v_p(x) := \text{ smallest index in the } p\text{-adic expansion of } x.$$

Observe: If x in $\mathbb{Q}_p$ is a nonzero square, then $v_p(x)$ is even.So our previous corollary becomes:

Proposition

A nonzero rational number $x \in \mathbb{Q}$ is a square if and only if it is a square in $\mathbb{R}$ and in each $\mathbb{Q}_p$.

This result is an example of what is called a *local-global principle*.

Local-global principles in theory

Definition

Roughly speaking, a *local-global principle* is a theorem of the form "statement P is true over $\mathbb{Q}$ if and only if it is true over each $\mathbb{Q}_p$ and over $\mathbb{R}$".

Local-global principles in theory

Definition

Roughly speaking, a *local-global principle* is a theorem of the form "statement P is true over $\mathbb{Q}$ if and only if it is true over each $\mathbb{Q}_p$ and over $\mathbb{R}$".

The terminology "local-global" can be explained as follows:

Local-global principles in theory

Definition

Roughly speaking, a *local-global principle* is a theorem of the form "statement P is true over $\mathbb{Q}$ if and only if it is true over each $\mathbb{Q}_p$ and over $\mathbb{R}$".

The terminology "local-global" can be explained as follows:

- What pertains to $\mathbb{Q}_p$ is "local" because you "focus" on one prime and forget the others.

Local-global principles in theory

Definition

Roughly speaking, a *local-global principle* is a theorem of the form "statement P is true over $\mathbb{Q}$ if and only if it is true over each $\mathbb{Q}_p$ and over $\mathbb{R}$".

The terminology "local-global" can be explained as follows:

• What pertains to $\mathbb{Q}_p$ is "local" because you "focus" on one prime and forget the others.

• What pertains to $\mathbb{Q}$ is "global" because in $\mathbb{Q}$ you see "the whole picture" (all primes at once).

Local-global principles in theory

Definition

Roughly speaking, a *local-global principle* is a theorem of the form "statement P is true over $\mathbb{Q}$ if and only if it is true over each $\mathbb{Q}_p$ and over $\mathbb{R}$".

The terminology "local-global" can be explained as follows:

• What pertains to $\mathbb{Q}_p$ is "local" because you "focus" on one prime and forget the others.

• What pertains to $\mathbb{Q}$ is "global" because in $\mathbb{Q}$ you see "the whole picture" (all primes at once).

The relevance of local-global principles is that many problems are easier to solve "locally" than "globally".

Local-global principles in theory

Definition

Roughly speaking, a *local-global principle* is a theorem of the form "statement P is true over $\mathbb{Q}$ if and only if it is true over each $\mathbb{Q}_p$ and over $\mathbb{R}$".

The terminology "local-global" can be explained as follows:

• What pertains to $\mathbb{Q}_p$ is "local" because you "focus" on one prime and forget the others.

• What pertains to $\mathbb{Q}$ is "global" because in $\mathbb{Q}$ you see "the whole picture" (all primes at once).

The relevance of local-global principles is that many problems are easier to solve "locally" than "globally". Whenever a local-global principle holds, the local study yields global information.

Local-global principles in practice

To illustrate a local-global principle, consider quadratic equations with coefficients in $\mathbb{Q}$:

$$q(x_1, \ldots, x_n) = 0.$$

Local-global principles in practice

To illustrate a local-global principle, consider quadratic equations with coefficients in $\mathbb{Q}$:

$$q(x_1, \ldots, x_n) = 0.$$

We shall restrict* to q *homogeneous*; this means that all monomials have degree 2.

Local-global principles in practice

To illustrate a local-global principle, consider quadratic equations with coefficients in $\mathbb{Q}$:

$$q(x_1, \ldots, x_n) = 0.$$

We shall restrict* to q *homogeneous*; this means that all monomials have degree 2. In other words, q is a *quadratic form*,

$$q(x_1, \ldots, x_n) = (x_1, \ldots, x_n) A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \qquad \forall (x_1, \ldots, x_n).$$

Local-global principles in practice

To illustrate a local-global principle, consider quadratic equations with coefficients in $\mathbb{Q}$:

$$q(x_1, \ldots, x_n) = 0.$$

We shall restrict* to q *homogeneous*; this means that all monomials have degree 2. In other words, q is a *quadratic form*,

$$q(x_1, \ldots, x_n) = (x_1, \ldots, x_n) A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \qquad \forall (x_1, \ldots, x_n).$$

In this case, we look for *nontrivial* solutions, i.e., we discard the solution $(x_1, \ldots, x_n) = (0, \ldots, 0)$.

Quadratic forms in summary

Two must-know things on quadratic forms (over any* field):

Quadratic forms in summary

Two must-know things on quadratic forms (over any* field):

(1) One can always assume q is in *diagonal form* $q(x_1, \ldots, x_n) = \sum a_i x_i^2$, up to a coordinate change.

Quadratic forms in summary

Two must-know things on quadratic forms (over any* field):

(1) One can always assume q is in *diagonal form* $q(x_1, \ldots, x_n) = \sum a_i x_i^2$, up to a coordinate change. (Think of "completing the square".)

Quadratic forms in summary

Two must-know things on quadratic forms (over any* field):

(1) One can always assume q is in *diagonal form* $q(x_1, \ldots, x_n) = \sum a_i x_i^2$, up to a coordinate change.
(Think of "completing the square".)

(2) By scaling the variables, one can "get rid of squares in the coefficients".

Quadratic forms in summary

Two must-know things on quadratic forms (over any* field):

(1) One can always assume q is in *diagonal form* $q(x_1, \ldots, x_n) = \sum a_i x_i^2$, up to a coordinate change. (Think of "completing the square".)

(2) By scaling the variables, one can "get rid of squares in the coefficients". This is dependent on the ground field.

Quadratic forms in summary

Two must-know things on quadratic forms (over any* field):

(1) One can always assume q is in *diagonal form* $q(x_1, \ldots, x_n) = \sum a_i x_i^2$, up to a coordinate change. (Think of "completing the square".)

(2) By scaling the variables, one can "get rid of squares in the coefficients". This is dependent on the ground field.

Examples

Consider

$$q(x, y, z, w) = x^2 + \frac{1}{4}y^2 + \frac{1}{2}z^2 - w^2.$$

Quadratic forms in summary

Two must-know things on quadratic forms (over any* field):

(1) One can always assume q is in *diagonal form* $q(x_1, \ldots, x_n) = \sum a_i x_i^2$, up to a coordinate change. (Think of "completing the square".)

(2) By scaling the variables, one can "get rid of squares in the coefficients". This is dependent on the ground field.

Examples

Consider

$$q(x, y, z, w) = x^2 + \frac{1}{4}y^2 + \frac{1}{2}z^2 - w^2.$$

- Put $Y = \frac{y}{2} \rightsquigarrow$ the second coefficient becomes 1.

Quadratic forms in summary

Two must-know things on quadratic forms (over any* field):

(1) One can always assume q is in *diagonal form* $q(x_1, \ldots, x_n) = \sum a_i x_i^2$, up to a coordinate change. (Think of "completing the square".)

(2) By scaling the variables, one can "get rid of squares in the coefficients". This is dependent on the ground field.

Examples

Consider

$$q(x, y, z, w) = x^2 + \frac{1}{4}y^2 + \frac{1}{2}z^2 - w^2.$$

- Put $Y = \frac{y}{2} \rightsquigarrow$ the second coefficient becomes 1.
- (E.g. over $\mathbb{R}$): Put $Z = \frac{z}{\sqrt{2}} \rightsquigarrow$ the third coefficient becomes 1.

Quadratic forms in summary

Two must-know things on quadratic forms (over any* field):

(1) One can always assume q is in *diagonal form* $q(x_1, \ldots, x_n) = \sum a_i x_i^2$, up to a coordinate change. (Think of "completing the square".)

(2) By scaling the variables, one can "get rid of squares in the coefficients". This is dependent on the ground field.

Examples

Consider

$$q(x, y, z, w) = x^2 + \frac{1}{4}y^2 + \frac{1}{2}z^2 - w^2.$$

- Put $Y = \frac{y}{2} \rightsquigarrow$ the second coefficient becomes 1.
- (E.g. over $\mathbb{R}$): Put $Z = \frac{z}{\sqrt{2}} \rightsquigarrow$ the third coefficient becomes 1.
- (E.g. over $\mathbb{C}$): Put $W = iw \rightsquigarrow$ the fourth coefficient becomes 1.

Standard forms locally and globally

More formally, the last observation tells us:

Standard forms locally and globally

More formally, the last observation tells us: *If we choose a system of representatives $\mathcal{R}$ for the quotient set $K^\times/K^{\times 2}$ ("nonzero elements modulo squares"),*

Standard forms locally and globally

More formally, the last observation tells us: *If we choose a system of representatives $\mathcal{R}$ for the quotient set $K^\times/K^{\times 2}$ ("nonzero elements modulo squares"), then any quadratic form over K can be put in the form*

$$q(x_1, \ldots, x_n) = \sum a_i x_i^2$$

where, for each i, $a_i \in \mathcal{R}$ or $a_i = 0$.

Standard forms locally and globally

More formally, the last observation tells us: *If we choose a system of representatives $\mathcal{R}$ for the quotient set $K^\times / K^{\times 2}$ ("nonzero elements modulo squares"), then any quadratic form over K can be put in the form*

$$q(x_1, \ldots, x_n) = \sum a_i x_i^2$$

where, for each i, $a_i \in \mathcal{R}$ or $a_i = 0$.

Example

(1) Over $\mathbb{R}$, the coefficients can be chosen to be in $\{+1, -1, 0\}$. (**Sylvester's law of inertia**)

Standard forms locally and globally

More formally, the last observation tells us: *If we choose a system of representatives $\mathcal{R}$ for the quotient set $K^\times/K^{\times 2}$ ("nonzero elements modulo squares"), then any quadratic form over K can be put in the form*

$$q(x_1, \ldots, x_n) = \sum a_i x_i^2$$

where, for each i, $a_i \in \mathcal{R}$ or $a_i = 0$.

Example

(1) Over $\mathbb{R}$, the coefficients can be chosen to be in $\{+1, -1, 0\}$. (**Sylvester's law of inertia**)

(2) Over $\mathbb{Q}$, we have $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} = \ldots$

Standard forms locally and globally

More formally, the last observation tells us: *If we choose a system of representatives $\mathcal{R}$ for the quotient set $K^\times/K^{\times 2}$ ("nonzero elements modulo squares"), then any quadratic form over K can be put in the form*

$$q(x_1, \ldots, x_n) = \sum a_i x_i^2$$

where, for each i, $a_i \in \mathcal{R}$ or $a_i = 0$.

Example

(1) Over $\mathbb{R}$, the coefficients can be chosen to be in $\{+1, -1, 0\}$. (**Sylvester's law of inertia**)

(2) Over $\mathbb{Q}$, we have $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} = \ldots$???

Standard forms locally and globally

More formally, the last observation tells us: *If we choose a system of representatives* $\mathcal{R}$ *for the quotient set* $K^\times/K^{\times 2}$ *("nonzero elements modulo squares"), then any quadratic form over* K *can be put in the form*

$$q(x_1, \ldots, x_n) = \sum a_i x_i^2$$

where, for each i*,* $a_i \in \mathcal{R}$ *or* $a_i = 0$*.*

Example

(1) Over $\mathbb{R}$, the coefficients can be chosen to be in $\{+1, -1, 0\}$. (**Sylvester's law of inertia**)

(2) Over $\mathbb{Q}$, we have $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} = \ldots$??? (infinite)

Standard forms locally and globally

More formally, the last observation tells us: *If we choose a system of representatives $\mathcal{R}$ for the quotient set $K^\times/K^{\times 2}$ ("nonzero elements modulo squares"), then any quadratic form over K can be put in the form*

$$q(x_1, \ldots, x_n) = \sum a_i x_i^2$$

where, for each i, $a_i \in \mathcal{R}$ or $a_i = 0$.

Example

(1) Over $\mathbb{R}$, the coefficients can be chosen to be in $\{+1, -1, 0\}$. (**Sylvester's law of inertia**)

(2) Over $\mathbb{Q}$, we have $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} = \ldots$??? (infinite)

(3) Over $K = \mathbb{Q}_p$, we have

Standard forms locally and globally

More formally, the last observation tells us: *If we choose a system of representatives $\mathcal{R}$ for the quotient set $K^\times/K^{\times 2}$ ("nonzero elements modulo squares"), then any quadratic form over K can be put in the form*

$$q(x_1, \ldots, x_n) = \sum a_i x_i^2$$

where, for each i, $a_i \in \mathcal{R}$ or $a_i = 0$.

Example

(1) Over $\mathbb{R}$, the coefficients can be chosen to be in $\{+1, -1, 0\}$. (**Sylvester's law of inertia**)

(2) Over $\mathbb{Q}$, we have $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} = \ldots$??? (infinite)

(3) Over $K = \mathbb{Q}_p$, we have

$$K^\times/K^{\times 2} \text{ has cardinality } = \begin{cases} 4, & p \neq 2, \\ 8, & p = 2. \end{cases}$$

Squares in $\mathbb{Q}_p$, $p \neq 2$

Squares in $\mathbb{Q}_p$, $p \neq 2$

Remark

(1) If x is a square in $\mathbb{Q}_p$, then its order $v_p(x)$ is even.

Squares in $\mathbb{Q}_p$, $p \neq 2$

Remark

(1) If x is a square in $\mathbb{Q}_p$, then its order $v_p(x)$ is even.

(2) When squaring, the leading coefficient gets "squared up to multiples of p".

Squares in $\mathbb{Q}_p$, $p \neq 2$

Remark

(1) If x is a square in $\mathbb{Q}_p$, then its order $v_p(x)$ is even.

(2) When squaring, the leading coefficient gets "squared up to multiples of p". The map

$$\{\text{leading coefficient of } x\} \mapsto \{\text{leading coefficient of } x^2\}$$

is a 2-to-1-map on the set $\{1, \dots, p-1\}$.

Squares in $\mathbb{Q}_p$, $p \neq 2$

Remark

(1) If x is a square in $\mathbb{Q}_p$, then its order $v_p(x)$ is even.

(2) When squaring, the leading coefficient gets "squared up to multiples of p". The map

$$\{\text{leading coefficient of } x\} \mapsto \{\text{leading coefficient of } x^2\}$$

is a 2-to-1-map on the set $\{1, \dots, p-1\}$.

Thus, for $x \in \mathbb{Q}_p$ nonzero, there are four possibilies:

Squares in $\mathbb{Q}_p$, $p \neq 2$

Remark

(1) If x is a square in $\mathbb{Q}_p$, then its order $v_p(x)$ is even.

(2) When squaring, the leading coefficient gets "squared up to multiples of p". The map

$$\{\text{leading coefficient of } x\} \mapsto \{\text{leading coefficient of } x^2\}$$

is a 2-to-1-map on the set $\{1, \ldots, p-1\}$.

Thus, for $x \in \mathbb{Q}_p$ nonzero, there are four possibilies:

	even order	odd order
a_ν square mod p		
a_ν nonsquare mod p		

Squares in $\mathbb{Q}_p$, $p \neq 2$

Remark

(1) If x is a square in $\mathbb{Q}_p$, then its order $v_p(x)$ is even.

(2) When squaring, the leading coefficient gets "squared up to multiples of p". The map

$$\{\text{leading coefficient of } x\} \mapsto \{\text{leading coefficient of } x^2\}$$

is a 2-to-1-map on the set $\{1, \ldots, p-1\}$.

Thus, for $x \in \mathbb{Q}_p$ nonzero, there are four possibilies:

	even order	odd order
a_ν square mod p	1	
a_ν nonsquare mod p		

Squares in $\mathbb{Q}_p$, $p \neq 2$

Remark

(1) If x is a square in $\mathbb{Q}_p$, then its order $v_p(x)$ is even.

(2) When squaring, the leading coefficient gets "squared up to multiples of p". The map

$$\{\text{leading coefficient of } x\} \mapsto \{\text{leading coefficient of } x^2\}$$

is a 2-to-1-map on the set $\{1, \ldots, p-1\}$.

Thus, for $x \in \mathbb{Q}_p$ nonzero, there are four possibilies:

	even order	odd order
a_ν square mod p	1	p
a_ν nonsquare mod p		

Squares in $\mathbb{Q}_p$, $p \neq 2$

Remark

(1) If x is a square in $\mathbb{Q}_p$, then its order $v_p(x)$ is even.

(2) When squaring, the leading coefficient gets "squared up to multiples of p". The map

$$\{\text{leading coefficient of } x\} \mapsto \{\text{leading coefficient of } x^2\}$$

is a 2-to-1-map on the set $\{1, \ldots, p-1\}$.

Thus, for $x \in \mathbb{Q}_p$ nonzero, there are four possibilies:

	even order	odd order
a_ν square mod p	1	p
a_ν nonsquare mod p	u	

Squares in $\mathbb{Q}_p$, $p \neq 2$

Remark

(1) If x is a square in $\mathbb{Q}_p$, then its order $v_p(x)$ is even.

(2) When squaring, the leading coefficient gets "squared up to multiples of p". The map

$$\{\text{leading coefficient of } x\} \mapsto \{\text{leading coefficient of } x^2\}$$

is a 2-to-1-map on the set $\{1, \ldots, p-1\}$.

Thus, for $x \in \mathbb{Q}_p$ nonzero, there are four possibilies:

	even order	odd order
a_ν square mod p	1	p
a_ν nonsquare mod p	u	up

Quadratic forms over $\mathbb{Q}_p$, $p \neq 2$

Fundamental technique: Solve for the 0-th coefficient and pull back up. (Hensel's Lemma)

Quadratic forms over $\mathbb{Q}_p$, $p \neq 2$

Fundamental technique: Solve for the 0-th coefficient and pull back up. (Hensel's Lemma)

We say that $q(x_1, \ldots, x_n)$ *represents* an element a of the ground field if the equation $q(x_1, \ldots, x_n) = a$ has a (nontrivial) solution.

Quadratic forms over $\mathbb{Q}_p$, $p \neq 2$

Fundamental technique: Solve for the 0-th coefficient and pull back up. (Hensel's Lemma)

We say that $q(x_1, \ldots, x_n)$ *represents* an element a of the ground field if the equation $q(x_1, \ldots, x_n) = a$ has a (nontrivial) solution.

Theorem

Let $q(x_1, \ldots, x_n) = \sum a_i x_i^2$.

(1) If $n = 2$ and a_1, a_2 have order 0, then q represents 1.

Quadratic forms over $\mathbb{Q}_p$, $p \neq 2$

Fundamental technique: Solve for the 0-th coefficient and pull back up. (Hensel's Lemma)

We say that $q(x_1, \ldots, x_n)$ *represents* an element a of the ground field if the equation $q(x_1, \ldots, x_n) = a$ has a (nontrivial) solution.

Theorem

Let $q(x_1, \ldots, x_n) = \sum a_i x_i^2$.

(1) If $n = 2$ and a_1, a_2 have order 0, then q represents 1. (all squares)

Quadratic forms over $\mathbb{Q}_p$, $p \neq 2$

Fundamental technique: Solve for the 0-th coefficient and pull back up. (Hensel's Lemma)

We say that $q(x_1, \ldots, x_n)$ *represents* an element a of the ground field if the equation $q(x_1, \ldots, x_n) = a$ has a (nontrivial) solution.

Theorem

Let $q(x_1, \ldots, x_n) = \sum a_i x_i^2$*.*

(1) If $n = 2$ *and* a_1*,* a_2 *have order* 0*, then* q *represents* 1*. (all squares)*

(2) If $n = 3$ *and* a_1*,* a_2*,* a_3 *have order* 0*, then* q *represents* 0*. By the general theory, it represents* *__all__* *elements of* $\mathbb{Q}_p$*.*

Quadratic forms over $\mathbb{Q}_p$, $p \neq 2$

Fundamental technique: Solve for the 0-th coefficient and pull back up. (Hensel's Lemma)

We say that $q(x_1, \ldots, x_n)$ *represents* an element a of the ground field if the equation $q(x_1, \ldots, x_n) = a$ has a (nontrivial) solution.

Theorem

Let $q(x_1, \ldots, x_n) = \sum a_i x_i^2$.

(1) If $n = 2$ and a_1, a_2 have order 0, then q represents 1. (all squares)

(2) If $n = 3$ and a_1, a_2, a_3 have order 0, then q represents 0. By the general theory, it represents <u>all</u> elements of $\mathbb{Q}_p$.

(3) If $n = 4$ and all a_i are nonzero, then q represents <u>all</u> elements of $\mathbb{Q}_p$ <u>except</u> in the case where each coefficient belongs to a different class in $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$. In this case, it represents all <u>nonzero</u> elements.

Quadratic forms over $\mathbb{Q}_p$, $p \neq 2$

Fundamental technique: Solve for the 0-th coefficient and pull back up. (Hensel's Lemma)

We say that $q(x_1, \ldots, x_n)$ *represents* an element a of the ground field if the equation $q(x_1, \ldots, x_n) = a$ has a (nontrivial) solution.

Theorem

Let $q(x_1, \ldots, x_n) = \sum a_i x_i^2$.

(1) If $n = 2$ and a_1, a_2 have order 0, then q represents 1. (all squares)

(2) If $n = 3$ and a_1, a_2, a_3 have order 0, then q represents 0. By the general theory, it represents all elements of $\mathbb{Q}_p$.

(3) If $n = 4$ and all a_i are nonzero, then q represents all elements of $\mathbb{Q}_p$ except in the case where each coefficient belongs to a different class in $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$. In this case, it represents all nonzero elements.

(4) If $n \geq 5$, then q represents all elements of $\mathbb{Q}_p$.

The Theorem of Minkowski and Hasse

The most famous instance of a local-global principle is the Theorem of Minkowski and Hasse on quadratic forms.

The Theorem of Minkowski and Hasse

The most famous instance of a local-global principle is the Theorem of Minkowski and Hasse on quadratic forms.

Theorem (Theorem of Minkowski and Hasse)

A quadratic form over $\mathbb{Q}$ in any number of variables represents 0 if and only if it does so over each $\mathbb{Q}_p$ and over $\mathbb{R}$.

The Theorem of Minkowski and Hasse

The most famous instance of a local-global principle is the Theorem of Minkowski and Hasse on quadratic forms.

Theorem (Theorem of Minkowski and Hasse)

A quadratic form over $\mathbb{Q}$ in any number of variables represents 0 if and only if it does so over each $\mathbb{Q}_p$ and over $\mathbb{R}$.

Corollary

(1) A quadratic form as above represents $a \in \mathbb{Q}$ if and only if it does so over each $\mathbb{Q}_p$ and over $\mathbb{R}$.

The Theorem of Minkowski and Hasse

The most famous instance of a local-global principle is the Theorem of Minkowski and Hasse on quadratic forms.

Theorem (Theorem of Minkowski and Hasse)

A quadratic form over $\mathbb{Q}$ in any number of variables represents 0 if and only if it does so over each $\mathbb{Q}_p$ and over $\mathbb{R}$.

Corollary

(1) A quadratic form as above represents $a \in \mathbb{Q}$ if and only if it does so over each $\mathbb{Q}_p$ and over $\mathbb{R}$.

(2) Two quadratic forms over $\mathbb{Q}$ are "the same" (isomorphic) if and only if they are "the same" over every $\mathbb{Q}_p$ and over $\mathbb{R}$ (which is trivial to check).

And now for something totally disconnected. . .

And now for something totally disconnected...

(i.e., some drawings on the blackboard explaining the topology of $\mathbb{Q}_p$)

Thank you for your attention!