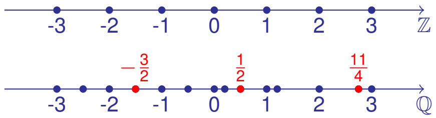
Chapter 5: Construction of the Real Numbers

February 18 & 20, 2014

Lecturer: Fan Yang

Rational Numbers

We now extend the set $\mathbb{Z}$ of integers to the set $\mathbb{Q}$ of rational numbers in much the same way as we extended ω to $\mathbb{Z}$.



Any rational number is equal to a fraction $\dfrac{a}{b}$, where $b \neq 0$. This can also be represented as an ordered pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}'$, where $\mathbb{Z}' = \mathbb{Z} \setminus \{0\}$.

The fractions

$$\frac{1}{2}, \quad \frac{-2}{-4}, \quad \frac{5}{10}, \ldots$$

represent the same rational number. In view of this, we cannot simply define $\frac{1}{2}_{\mathbb{Q}} := (1, 2)$ or $\frac{1}{2}_{\mathbb{Q}} := (-2, -4)$, for $(1, 2) \neq (-2, -4)$. Instead, we define an equivalence relation $\sim$ for which

$$(1, 2) \sim (-2, -4) \sim (5, 10) \sim \ldots,$$

and let $\frac{1}{2}_{\mathbb{Q}} := [(1, 2)] = [(-2, -4)] = [(5, 10)] = \ldots.$

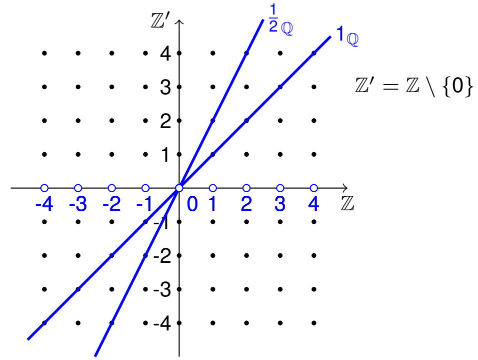
In general, we want: $(a, b) \sim (c, d)$ iff $\dfrac{a}{b} = \dfrac{c}{d}$ iff $ad = cb$.

Definition 5.8

Define an equivalence relation $\sim$ on $\mathbb{Z} \times \mathbb{Z}'$ as

$$(a, b) \sim (c, d) \quad \text{iff} \quad ad = cb \quad [\text{ (informally) iff } \frac{a}{b} = \frac{c}{d}].$$

Define the set $\mathbb{Q}$ of rational numbers as $\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}')/_{\sim}$.



For example,

- $\frac{1}{2}_{\mathbb{Q}} = [(1,2)] = [(-2,-4)] = \{(1,2),(-2,-4),(5,10),\ldots\}$,
- For any $[(a,b)] \in \mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}')/_\sim$, we have $(c,0) \notin [(a,b)]$ for any $c \in \mathbb{Z}$.
- $1_{\mathbb{Q}} = [(1,1)] = [(a,a)]$ for all nonzero integer a.
- $0_{\mathbb{Q}} = [(0,1)] = [(0,a)]$ for all nonzero integer a.
- $0_{\mathbb{Q}} \neq 1_{\mathbb{Q}}$, since $0 \cdot 1 \neq 1 \cdot 1 \implies (0,1) \not\sim (1,1)$.

Theorem 5QA

The relation $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}'$.

Proof. Let $(a,b),(c,d),(e,f) \in \mathbb{Z} \times \mathbb{Z}'$.

Reflexivity: $ab = ab \implies (a,b) \sim (a,b)$.

Symmetricity:

$$(a,b) \sim (c,d) \implies ad = cb \implies cb = ad \implies (c,d) \sim (a,b).$$

Transitivity:

$$\begin{aligned} & (a,b) \sim (c,d) \text{ and } (c,d) \sim (e,f) \\ & \implies ad = cb \text{ and } cf = ed \\ & \implies fad = fcb \text{ and } cfb = edb \\ & \implies fad = edb \\ (\because d \neq 0) & \implies af = eb \implies (a,b) \sim (e,f). \end{aligned}$$

□

Informally, addition on $\mathbb{Q}$ acts as $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$.

Note: Since $b, d \neq 0$, the denominator $bd \neq 0$.

Definition 5.9 (Addition)

Define the addition operation $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ on $\mathbb{Q}$ as

$$[(a,b)] + [(c,d)] = [(ad+cb, bd)].$$

Example 5.6: Prove $\frac{3}{4}_{\mathbb{Q}} + \left(-\frac{1}{4}_{\mathbb{Q}}\right) = \frac{1}{2}_{\mathbb{Q}}$ in $\mathbb{Q}$.

Proof.
$$\begin{aligned} \frac{3}{4}_{\mathbb{Q}} + \left(-\frac{1}{4}_{\mathbb{Q}}\right) & = [(3,4)] + [(-1,4)] \\ & = [(3 \cdot 4 + (-1) \cdot 4, 4 \cdot 4)] \\ & = [(8,16)] \\ & = \frac{1}{2}_{\mathbb{Q}}. \end{aligned}$$

□

We check that $+$ is well-defined.

Lemma 5QB

If $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, then

$$(ad+cb, bd) \sim (a'd' + c'b', b'd').$$

Proof. Since $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, we have that

$$ab' = a'b \quad \text{and} \quad cd' = c'd.$$

It follows that

$$\begin{aligned} & ab'dd' = a'bdd' \quad \text{and} \quad cd'bb' = c'dbb' \\ \implies & ab'dd' + cd'bb' = a'bdd' + c'dbb' \\ \implies & (ad+cb)b'd' = (a'd' + c'b')bd \\ \implies & (ad+cb, bd) \sim (a'd' + c'b', b'd'). \end{aligned}$$

□

Theorem 5QC

(a) Let $q, r, s \in \mathbb{Q}$.
(associative law) $(q+r)+s = q+(r+s)$,
(commutative law) $r+s = s+r$.

(b) $0_{\mathbb{Q}} = [(0,1)]$ *is the additive identity:* $r + 0_{\mathbb{Q}} = r$ *for all* $r \in \mathbb{Q}$.

(c) For any $r \in \mathbb{Q}$, there exists a unique $s \in \mathbb{Q}$ such that $r + s = 0_{\mathbb{Q}}$. The unique s is called the additive inverse of r, denoted by $-r$.

Proof. We only prove (c). Let $r = [(a,b)]$. Take $s = [(-a,b)]$. Then

$$r + s = [(a,b)] + [(-a,b)] = [(ab + (-a)b, bb)] = [(0, bb)] = 0_{\mathbb{Q}}.$$

For uniqueness, assume $s' \in \mathbb{Q}$ is also an additive inverse of r. Then

$$s' = s' + 0_{\mathbb{Q}} = s' + (r+s) = (s'+r)+s = 0_{\mathbb{Q}} + s = s.$$

□

From the above proof, we see the following:

- $-[(a,b)] = [(-a,b)]$.
- Subtraction operation $- : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ can be defined as
  $$r - s := r + (-s).$$

Informally, multiplication on $\mathbb{Q}$ acts as

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Definition 5.10 (Multiplication)

Define Multiplication operation $\cdot$ on $\mathbb{Q}$ as

$$[(a,b)] \cdot [(c,d)] = [(ac, bd)].$$

Example 5.7: $1_{\mathbb{Q}} = [(1,1)]$ is the multiplicative identity, that is, $r \cdot 1_{\mathbb{Q}} = r$ for all $r \in \mathbb{Q}$.

Proof. Let $r = [(a,b)]$. Then

$$r \cdot 1_{\mathbb{Q}} = [(a,b)] \cdot [(1,1)] = [(a \cdot 1, b \cdot 1)] = [(a,b)] = r.$$

□

It is also easy to check that $r \cdot 0_{\mathbb{Q}} = 0_{\mathbb{Q}}$ (exercise).

We check that $\cdot$ is well-defined.

Lemma 5QD

If $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, then

$$(ac, bd) \sim (a'c', b'd').$$

Proof. Since $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, we have that

$$ab' = a'b \quad \text{and} \quad cd' = c'd.$$

Multiplying both sides of the above two equalities yields

$$ab'cd' = a'bc'd,$$

i.e., $acb'd' = a'c'bd$, which means $(ac, bd) \sim (a'c', b'd')$. □

Theorem 5QE

Let $q, r, s \in \mathbb{Q}$.
(associative law) $(q \cdot r) \cdot s = q \cdot (r \cdot s)$,
(commutative law) $r \cdot s = s \cdot r$.
(distributive law) $q \cdot (r+s) = q \cdot r + q \cdot s$.

Proof. We only prove distributive law. Let

$$q = [(a,b)], \quad r = [(c,d)], \quad s = [(e,f)].$$

where $b \neq 0$, $d \neq 0$ and $f \neq 0$. Then

$$q \cdot (r+s) = [(a,b)] \cdot ([(c,d)] + [(e,f)])$$
$$= [(a,b)] \cdot [(cf + ed, df)] = [(acf + aed, bdf)]$$

and

$$q \cdot r + q \cdot s = [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)]$$
$$= [(ac, bd)] + [(ae, bf)] = [(acbf + aebd, bdbf)].$$

Hence $q \cdot (r+s) = q \cdot r + q \cdot s$. □

Theorem 5QF

For every nonzero $r \in \mathbb{Q}$, there is a unique nonzero $q \in \mathbb{Q}$ such that $r \cdot q = 1_{\mathbb{Q}}$.
The unique q is called the multiplicative inverse of r, denoted by r^{-1}.

Proof. Let $r = [(a, b)]$. Take $q = [(b, a)]$. Since $a, b \neq 0$, q is a nonzero rational number. We have that

$$r \cdot q = [(a, b)] \cdot [(b, a)] = [(ab, ba)] = 1_{\mathbb{Q}}.$$

For uniqueness, if s is another multiplicative inverse of r, then

$$s = s \cdot 1_{\mathbb{Q}} = s \cdot (r \cdot q) = (s \cdot r) \cdot q = 1_{\mathbb{Q}} \cdot q = q.$$

□

From the above proof it follows that if $a, b \neq 0$, then $[(a, b)]^{-1} = [(b, a)]$.

Definition 5.11 (Division)

For any $s, r \in \mathbb{Q}$, if $r \neq 0_{\mathbb{Q}}$, then define $s \div r := s \cdot r^{-1}$.

That is, if $c \neq 0$ and $d \neq 0$, then

$$[(a, b)] \div [(c, d)] = [(a, b)] \cdot [(d, c)] = [(ad, bc)].$$

Corollary 5QG

If r and s are nonzero rational numbers, then $r \cdot s$ is also nonzero.

Proof. Since r and s are nonzero, by Theorem 5QF, their multiplicative inverses exist. If $r \cdot s = 0_{\mathbb{Q}}$, then

$$(r \cdot s) \cdot (s^{-1} \cdot r^{-1}) = 0_{\mathbb{Q}} \cdot (s^{-1} \cdot r^{-1}),$$

which gives $1_{\mathbb{Q}} = 0_{\mathbb{Q}}$. A contradiction. □

Informally, the ordering $<$ on $\mathbb{Q}$ satisfies

$$\frac{a}{b} < \frac{c}{d} \quad \text{iff} \quad ad < cb$$

as long as $b, d > 0$. Because $\frac{a}{b} = \frac{-a}{-b}$, every rational number can be represented by some fraction with a positive denominator.

Definition 5.12 (Ordering)

Define an ordering $<$ on $\mathbb{Q}$ as: for any two rationals $[(a, b)]$, $[(c, d)]$ with $b, d > 0$,

$$[(a, b)] < [(c, d)] \quad \text{iff} \quad ad < cb.$$

Example 5.8: Prove: $-\frac{1}{3}_{\mathbb{Q}} < 0_{\mathbb{Q}}$.

Proof. Note that $0_{\mathbb{Q}} = [(0, 1)]$ and $-\frac{1}{3}_{\mathbb{Q}} = [(-1, 3)]$. Since

$$(-1) \cdot 1 = -1 < 0 = 0 \cdot 3,$$

we conclude that $-\frac{1}{3}_{\mathbb{Q}} < 0_{\mathbb{Q}}$. □

We need to check that $<$ is well-defined.

Lemma 5QH

Let $b, b', d, d' > 0$. If $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then

$$ad < cb \quad \text{iff} \quad a'd' < c'd'.$$

Proof. Since $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, we have that

$$ab' = a'b \quad \text{and} \quad cd' = c'd,$$

which implies that

$$\begin{aligned} ad < cb &\iff adb'd' < cbb'd' \text{ (since } b'd' > 0) \\ &\iff a'bdd' < c'dbb' \text{ (by assumption)} \\ &\iff a'd' < c'b' \text{ (since } bd > 0). \end{aligned}$$

□

Lemma 5QI

The relation $<$ is a linear ordering on $\mathbb{Q}$.

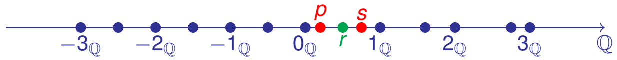
Proof. It suffices to check that $<$ is a transitive relation that satisfies trichotomy on $\mathbb{Q}$. We show the transitivity on blackboard. It remains to show trichotomy, which means that for any two rationals $r = [(a, b)]$ and $s = [(c, d)]$ with $b, d > 0$, exactly one of the following three alternatives holds:

$$r < s, \quad r = s, \quad s < r.$$

That is, exactly one of the following holds:

$$ad < cb, \quad ad = cb, \quad cb < ad.$$

But this follows from the trichotomy of $<$ in $\mathbb{Z}$. □



Fact: The ordering $<$ on $\mathbb{Q}$ is dense, i.e., for any $p, s \in \mathbb{Q}$,

$$p < s \Longrightarrow \exists r \in \mathbb{Q}(p < r < s).$$

The proof of this fact is left as an exercise.

Definition 5.13

A rational r is called positive iff $0_{\mathbb{Q}} < r$; negative iff $r < 0_{\mathbb{Q}}$.

The trichotomy of $<$ implies that exactly one of the following holds:

$$r \text{ is positive}, \quad r = 0_{\mathbb{Q}}, \quad r \text{ is negative}.$$

Definition 5.14 (absolute value)

Define the absolute value $|r|$ of a rational r by

$$|r| = \begin{cases} r, & \text{if } 0_{\mathbb{Q}} \le r; \\ -r, & \text{if } r < 0_{\mathbb{Q}}. \end{cases}$$

For example:

- $|-\frac{1}{3}_{\mathbb{Q}}| = |[(-1, 3)]| = -[(-1, 3)] = [(-(-1), 3)] = [(1, 3)] = \frac{1}{3}_{\mathbb{Q}}$.
- $0_{\mathbb{Q}} \le |r|$ for every $r \in \mathbb{Q}$.

Theorem 5QJ

Let $r, s, t \in \mathbb{Q}$.

(i) $r < s \iff r + t < s + t$.

(ii) *If $0_{\mathbb{Q}} < t$, then $r < s \iff r \cdot t < s \cdot t$.*

Proof. We only prove (i). Let

$$r = [(a, b)], \quad s = [(c, d)] \quad \text{and} \quad t = [(e, f)],$$

where $a, b, c, d, e, f \in \mathbb{Z}$ with $0 < b, d, f$. Then

$$\begin{aligned} r + t < s + t &\iff [(a, b)] + [(e, f)] < [(c, d)] + [(e, f)] \\ &\iff [(af + eb, bf)] < [(cf + ed, df)] \\ &\iff (af + eb)df < (cf + ed)bf \quad (\text{since } 0 < df, bf) \\ &\iff afdf + ebdf < cfbf + edbf \\ &\iff afdf < cfbf \\ &\iff ad < cb \quad (\text{since } 0 < ff) \\ &\iff r < s. \end{aligned}$$

□

Theorem 5QK

Let $r, s, t \in \mathbb{Q}$.

(i) $r + t = s + t \Longrightarrow r = s$

(ii) *$r \cdot t = s \cdot t$ and $t \ne 0 \Longrightarrow r = s$.*

Proof. For (i), we have that

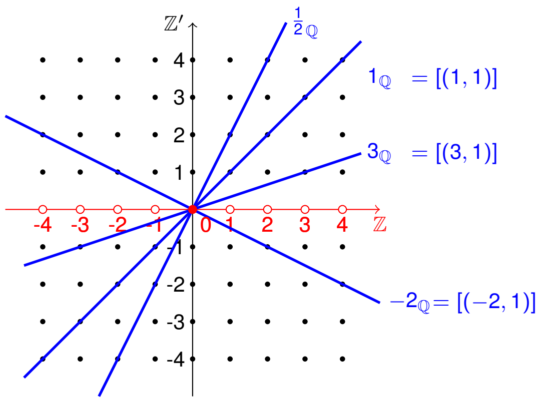
$$r+t = s+t \Longrightarrow (r+t)+(-t) = (s+t)+(-t) \Longrightarrow r+0_{\mathbb{Q}} = s+0_{\mathbb{Q}} \Longrightarrow r = s.$$

For (ii), since $t \ne 0$, the multiplicative inverse t^{-1} exists, thus

$$r \cdot t = s \cdot t \Longrightarrow (r \cdot t) \cdot (t^{-1}) = (s \cdot t) \cdot (t^{-1}) \Longrightarrow r \cdot 1_{\mathbb{Q}} = s \cdot 1_{\mathbb{Q}} \Longrightarrow r = s.$$

□

By our construction, the set $\mathbb{Z}$ is not actually a subset of the set $\mathbb{Q}$. However, $\mathbb{Q}$ has a subset that is "just like" $\mathbb{Z}$.



The function f defined as follows is an "isomorphic embedding" of the structure $\langle \mathbb{Z}, +, \cdot, < \rangle$ into the structure $\langle \mathbb{Q}, +, \cdot, < \rangle$.

Theorem 5ZL

Define a function $f : \mathbb{Z} \to \mathbb{Q}$ by taking

$$f(a) = [(a, 1)].$$

The function f is one-to-one and preserves operations and order: for any $a, b \in \mathbb{Z}$,

(a) $f(a + b) = f(a) + f(b)$;

(b) $f(a \cdot b) = f(a) \cdot f(b)$;

(c) $a < b$ iff $f(a) < f(b)$.

Proof. We first show that f is one-to-one. We have that

$$f(a) = f(b) \implies [(a,1)] = [(b,1)] \implies (a,1) \sim (b,1) \implies a \cdot 1 = b \cdot 1 \implies a = b.$$

For (a), $f(a + b) = [(a + b, 1)] = [(a,1)] + [(b,1)] = f(a) + f(b)$.

For (b), $f(a \cdot b) = [(a \cdot b, 1)] = [(a,1)] \cdot [(b,1)] = f(a) \cdot f(b)$.

For (c), $a < b$ iff $a \cdot 1 < b \cdot 1$ iff $[(a,1)] < [(b,1)]$ iff $f(a) < f(b)$. □

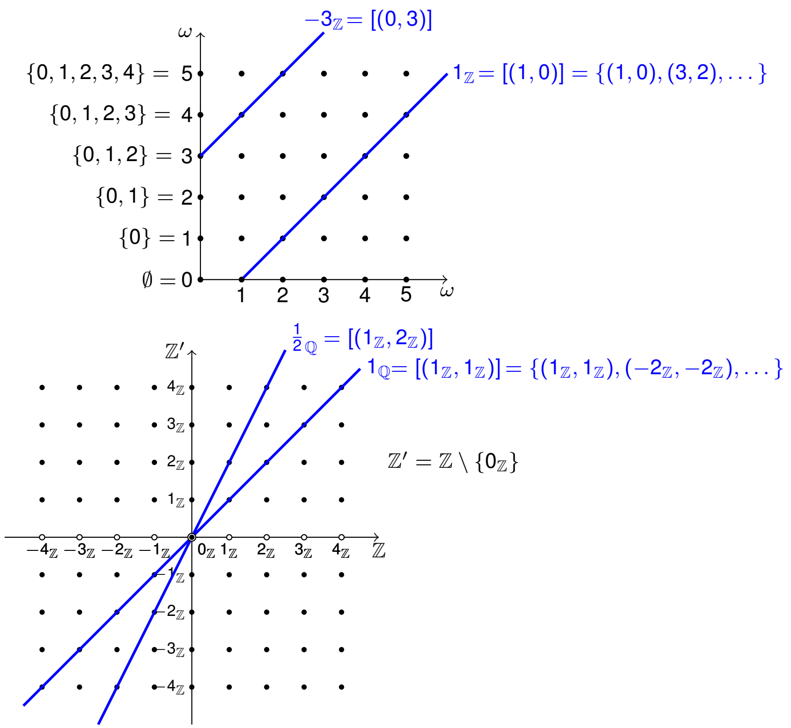
Intuitively, we let $\frac{1}{2}_{\mathbb{Q}} = [(2,4)] = [(3,6)] = \ldots$ because $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \ldots$.

Example 5.9: For any $a, b \in \mathbb{Z}$, if $b \neq 0$, then

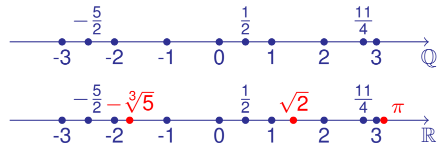
$$f(a) \div f(b) = [(a, b)].$$

Proof.
$$\begin{aligned} f(a) \div f(b) &= [(a,1)] \div [(b,1)] \\ &= [(a,1)] \cdot [(b,1)]^{-1} \\ &= [(a,1)] \cdot [(1,b)] \\ &= [(a,b)]. \end{aligned}$$
□

Real Numbers

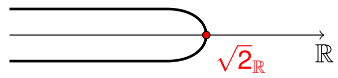


In this section, we will extend the set $\mathbb{Q}$ of rational numbers to the set $\mathbb{R}$ of real numbers.



An integer is named by a pair of natural numbers, and a rational number is named by a pair of integers. However, we will see in Chapter 6 that there are more real numbers than pairs of rational numbers. So it is not possible to name every real number by a pair of rational numbers.

Loosely speaking, we will *in effect* define a real number x to be the set of all rationals smaller than x.



Informally, $\sqrt{2}_{\mathbb{R}} = \{r \in \mathbb{Q} \mid r < \sqrt{2}\}$.

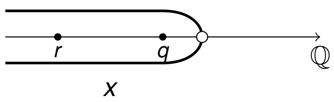
Definition 5.14 (Dedekind Cut)

A Dedekind cut is a non-empty proper subset x of $\mathbb{Q}$ such that

(i) *x is closed downwards, i.e., for all $q, r \in \mathbb{Q}$,*

$$q \in x \text{ and } r < q \Longrightarrow r \in x.$$

(ii) *x has no greatest element, i.e., there is no $r \in x$ such that $q \leq r$ for all $q \in x$.*



Note: None of $\emptyset$ and $\mathbb{Q}$ is a Dedekind cut, although they are both closed downwards and have no greatest element.

- $\mathbb{Q}$ has no greatest element, since for all $r \in \mathbb{Q}$, we have that $r + 1_{\mathbb{Q}} \in \mathbb{Q}$ and $r < r + 1_{\mathbb{Q}}$.

Definition 5.15

The set $\mathbb{R}$ of real numbers is the set of all Dedekind cuts.
That is, a real number is a Dedekind cut.

Example 5.10: The set $0_{\mathbb{R}} := \{r \in \mathbb{Q} \mid r < 0\}$ is a Dedekind cut, thus a real number.

Proof.

- $0_{\mathbb{R}} \neq \emptyset$, since e.g. $-1 \in 0_{\mathbb{R}}$.
- $0_{\mathbb{R}} \neq \mathbb{Q}$, since e.g. $0 \notin 0_{\mathbb{R}}$.
- For any $q, r \in \mathbb{Q}$, $\quad r < q \in 0_{\mathbb{R}} \Longrightarrow r < q < 0 \Longrightarrow r \in 0_{\mathbb{R}}$.
- For any $r \in 0_{\mathbb{R}}$, we have $r < 0$. Since $\mathbb{Q}$ is dense, there exists $q \in \mathbb{Q}$ such that $r < q < 0$, thus $q \in 0_{\mathbb{R}}$. □

Example 5.11: By a similar argument with the above, given any $q_0 \in \mathbb{Q}$, the set

$$q_{0\mathbb{R}} := \{r \in \mathbb{Q} \mid r < q_0\}$$

is a Dedekind cut, thus a real number.
In particular, $1_{\mathbb{R}} = \{r \in \mathbb{Q} \mid r < 1\}$ is a real number.