University of Toronto – MAT246H1-S – LEC0201/9201 – Winter 2021

Concepts in Abstract Mathematics

6 - The rationals and the reals

Jean-Baptiste Campesato

Positive rational numbers $\frac{p}{q}$ are systematically studied in Euclid's elements (circa 300BC), but they already appeared in ancient Egyptian mathematical writings.
In this chapter we are going to formally construct the set $\mathbb{Q}$ of rational numbers. The basic idea would be to set

$$\mathbb{Q} = \left\{ \frac{p}{q} \ : \ p \in \mathbb{Z},\, q \in \mathbb{Z} \setminus \{0\} \right\}$$

as it is often written in elementary introductions to mathematics. Nonetheless that's not a fully satisfactory definition since a same rational number may have different quotient expressions, for instance we want to have $\frac{10}{14} = \frac{5}{7}$. In order to formally solve this issue we are going to introduce the notion of *equivalence classes* and *quotient sets*.

The oldest known texts referring to irrational numbers are the Śulbasūtras. They contain the fact that the diagonal of a square sacrificial altar[1] is uncommensurable with the side length (i.e. the side and the diagonal can't be integral multiples of another length).

The Pythagorean Hippasus of Metapontum (circa 500BC) is often credited to have discovered the first proof of irrationality (it is known for sure that Pythagoreans were aware that $\sqrt{2}$ and φ are irrational, but there is a lot of confusion about the first author divulging irrationality, probably because of the subsequent damages to the dogma of the Pythagorean school). In ancient Greece, mathematics had a geometric flavour with a focus on constructions: therefore that was a geometric proof of uncommensurability (I will give an example later in this chapter).

There are several tales concerning the fate of the discoverer of uncommensurable lengths. In the most favorable version, he was expelled for his impiety (it was Pythagorean dogma that lengths are commensurable, and more generally that all the things in the world are commensurable, such as melodic intervals). In other versions, the discoverer was sentenced to death by drowning[2]. That was for sure the beginning of a deep philosophical crisis.

The second part of this chapter is devoted to the set $\mathbb{R}$ of real numbers. It allows us to take these irrational numbers into account. I will give several proofs of irrationality (disclaimer: no ancient greek philosopher has been harmed during the preparation of this text).

Contents

[1] Irrational numbers seem to always appear in a deadly context...
[2] I warned you that irrational numbers seem to always appear under deadly circumstances.

1 Equivalence classes

Recall that a binary relation $\sim$ on a set E is an *equivalence relation* if
(i) $\forall x \in E,\ x \sim x$ (*reflexivity*)
(ii) $\forall x, y \in E,\ x \sim y \implies y \sim x$ (*symmetry*)
(iii) $\forall x, y, z \in E,\ \big(x \sim y \text{ and } y \sim z\big) \implies x \sim z$ (*transitivity*)

In what follows, we fix E a set together with an equivalence relation $\sim$ on it. We define the *equivalence class of* $x \in E$ by

$$[x] = \{y \in E \ :\ x \sim y\}$$

and we say that x is a *representative* of $[x]$.
We may easily prove that equivalence classes satisfy the following properties:

- $\forall x \in E,\ x \in [x]$
- $\forall x, y \in E,\ x \sim y \Leftrightarrow [x] = [y]$
- $\forall x, y \in E,\ [x] = [y]$ or $[x] \cap [y] = \varnothing$

Proof.

- Let $x \in E$. Since $x \sim x$, we have that $x \in [x]$.
- Let $x, y \in E$.
  $\Rightarrow$ Assume that $x \sim y$. Let $z \in [x]$, then $x \sim z$. By transitivity $y \sim z$ so that $z \in [y]$.
  We proved that $[x] \subset [y]$. We may similarly prove that $[y] \subset [x]$. Hence $[x] = [y]$.
  $\Leftarrow$ Assume that $[x] = [y]$. Then $x \in [x] = [y]$, so $y \sim x$ (and thus $x \sim y$).
- Let $x, y \in E$. Assume that $[x] \cap [y] \neq \varnothing$, then there exists $z \in [x] \cap [y]$.
  Therefore $x \sim z$ and $y \sim z$. By transitivity, we get that $x \sim y$, thus $[x] = [y]$.

■

The set

$$E/\!\sim \ := \{[x] \ :\ x \in E\}$$

of equivalence classes of $\sim$ is called the *quotient set* of E for $\sim$.
An element of $E/\!\sim$ is a subset of E made of elements which are all equivalent for $\sim$.
According to the above properties the elements of $E/\!\sim$ form a partition of E:

$$E = \bigsqcup_{S \in E/\sim} S$$

The idea is that we want to identify all the elements which are equivalent: $x \sim y$ becomes $[x] = [y]$ in $E/\!\sim$.
That's a very convenient tool to construct new sets from already constructed ones.

Example 1. For instance $\mathbb{Z}/\!\mod 6$ contains 6 equivalence classes:

- $[0] = \{n \in \mathbb{Z} \ :\ n \equiv 0 \pmod 6\} = \{\dots, -12, -6, 0, 6, 12, \dots\}$
- $[1] = \{n \in \mathbb{Z} \ :\ n \equiv 1 \pmod 6\} = \{\dots, -11, -5, 1, 7, 13, \dots\}$
- $[2] = \{n \in \mathbb{Z} \ :\ n \equiv 2 \pmod 6\} = \{\dots, -10, -4, 2, 8, 14, \dots\}$
- $[3] = \{n \in \mathbb{Z} \ :\ n \equiv 3 \pmod 6\} = \{\dots, -9, -3, 3, 9, 15, \dots\}$
- $[4] = \{n \in \mathbb{Z} \ :\ n \equiv 4 \pmod 6\} = \{\dots, -8, -2, 4, 10, 16, \dots\}$
- $[5] = \{n \in \mathbb{Z} \ :\ n \equiv 5 \pmod 6\} = \{\dots, -7, -1, 5, 11, 17, \dots\}$

Note that -5, 1 and 7 are representatives of $[-5] = [1] = [7]$.
Congruences become an actual equality in $\mathbb{Z}/\!\mod 6$: $a \equiv b \pmod 6 \Leftrightarrow [a] = [b]$.
In this example, it is easy to see that the equivalence classes form a partition of $\mathbb{Z} = [0] \sqcup [1] \sqcup [2] \sqcup [3] \sqcup [4] \sqcup [5]$.
Indeed, an integer $n \in \mathbb{Z}$ is an element of exactly one of the equivalence classes (depending on its remainder for the Euclidean division by 6).

Remark 2. An equivalence relation is entirely characterized by its equivalence classes.
Indeed if we have a partition $E = \bigsqcup_{i\in I} S_i$ then

$$x \sim y \Leftrightarrow (\exists i \in I,\ x, y \in S_i)$$

defines an equivalence relation on E.

2 Rational numbers

Proposition 3. *The relation $\sim$ on $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$ defined by*

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc$$

is an equivalence relation.

Proof.
- *Reflexivity.* Let $(a,b) \in \mathbb{Z}\times\mathbb{Z}\setminus\{0\}$ then $ab = ba$ so that $(a,b) \sim (a,b)$.
- *Symmetry.* Let $(a,b),(c,d) \in \mathbb{Z}\times\mathbb{Z}\setminus\{0\}$. Assume that $(a,b) \sim (c,d)$ then $ad = bc$.
  Thus $cb = da$, i.e. $(c,d) \sim (a,b)$.
- *Transitivity.* Let $(a,b),(c,d),(e,f) \in \mathbb{Z}\times\mathbb{Z}\setminus\{0\}$. Assume that $(a,b) \sim (c,d)$ and that $(c,d) \sim (e,f)$.
  Then $ad = bc$ and $cf = de$. Therefore $adf = bcf = bde$.
  Since $d \neq 0$, by cancellation, $af = be$, i.e. $(a,b) \sim (e,f)$.

■

Definition 4. We define the set of *rational numbers* by $\mathbb{Q} \coloneqq (\mathbb{Z}\times\mathbb{Z}\setminus\{0\})/\sim$ and we denote the equivalence class of $(a,b) \in \mathbb{Z}\times\mathbb{Z}\setminus\{0\}$ by $\frac{a}{b} \coloneqq [(a,b)]$.

Remark 5. Note that $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$.

Remark 6. With the above definition, we may formally write that $\frac{12}{14} = \frac{6}{7}$: indeed $(12,14) \sim (6,7)$ since $12\times 7 = 84 = 14\times 6$.

Remark 7. We defined a rational number as a set of couples, but what really matters is how the usual operations and the order are defined on rational numbers $\frac{a}{b} \in \mathbb{Q}$.

Remark 8. Note that for $(a,b) \in \mathbb{Z}\times\mathbb{Z}\setminus\{0\}$, we have $\frac{-a}{b} = \frac{a}{-b}$. Hence we set $-\frac{a}{b} \coloneqq \frac{-a}{b} = \frac{a}{-b}$.

Remark 9. Note that $\frac{a}{b} = 0 \Leftrightarrow a = 0$ and that if $\frac{a}{b} = \frac{a'}{b'} \neq 0$ then $\frac{b}{a} = \frac{b'}{a'}$.
Hence, if $x = \frac{a}{b} \neq 0$, we set $x^{-1} \coloneqq \frac{b}{a}$ which doesn't depend on the representative of x.

Proposition 10. *Given $x \in \mathbb{Q}$, there exists a unique couple $(a,b) \in \mathbb{Z}\times\mathbb{N}\setminus\{0\}$ such that $x = \frac{a}{b}$ and $\gcd(a,b) = 1$. Then we say that $x = \frac{a}{b}$ is written in* lowest form.

Proof. Let $x \in \mathbb{Q}$.
Existence. There exist $\alpha \in \mathbb{Z}$ and $\beta \in \mathbb{Z}\setminus\{0\}$ such that $x = \frac{\alpha}{\beta}$.
Write $d = \gcd(\alpha,\beta)$, then there exist $a \in \mathbb{Z}$ and $b \in \mathbb{Z}\setminus\{0\}$ such that $\alpha = da$ and $\beta = db$.
We have $d = \gcd(\alpha,\beta) = \gcd(da,db) = d\gcd(a,b)$, so $\gcd(a,b) = 1$.
Besides $\frac{\alpha}{\beta} = \frac{\operatorname{sign}(b)a}{|b|}$ since $\operatorname{sign}(b)a\beta = \operatorname{sign}(b)adb = |b|da = |b|\alpha$.
Uniqueness. Assume that $\frac{a}{b} = \frac{a'}{b'}$ where $a,a' \in \mathbb{Z}$, $b,b' \in \mathbb{N}\setminus\{0\}$, $\gcd(a,b) = 1$, $\gcd(a',b') = 1$.
Then $ab' = a'b$. By Gauss' lemma, since $b|ab'$ and $\gcd(a,b) = 1$, we get that $b|b'$. Similarly $b'|b$.
Since $b|b'$ and $b'|b$, we get $|b| = |b'|$, and thus $b = b'$.
Then, using the cancellation rule, $ab' = a'b$ gives $a = a'$ since $b = b' \neq 0$. ■

Remark 11. Note that the function $\varphi : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Q} \\ n & \mapsto & \frac{n}{1} \end{array}$ is injective. Indeed, $\forall n, m \in \mathbb{Z}$, $\frac{n}{1} = \frac{m}{1} \Leftrightarrow n = m$.
Therefore we may see $\mathbb{Z}$ as a subset of $\mathbb{Q}$ by setting $n \coloneqq \frac{n}{1} \in \mathbb{Q}$ for $n \in \mathbb{Z}$.
More formally, $\varphi(\mathbb{Z}) \subset \mathbb{Q}$ and we may identify $\mathbb{Z}$ with $\varphi(\mathbb{Z})$ since $\varphi : \mathbb{Z} \to \varphi(\mathbb{Z})$ is bijective.

Proposition 12. *The addition* $+ : \begin{array}{ccc} \mathbb{Q} \times \mathbb{Q} & \to & \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) & \mapsto & \frac{ad+bc}{bd} \end{array}$ *is well-defined.*

Proof. We need to prove that the addition doesn't depend on the choice of the representatives,
i.e. that if $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$.
Assume that $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$, i.e. $ab' = ba'$ and $cd' = dc'$.
Therefore $(ad + bc)(b'd') = adb'd' + bcb'd' = ba'dd' + dc'bb' = (a'd' + b'c')(bd)$, i.e. $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$. ∎

Remark 13. Note that the addition defined on $\mathbb{Q}$ is compatible with the one on $\mathbb{Z}$.
Indeed, if $m, n \in \mathbb{Z}$ then $\frac{m}{1} + \frac{n}{1} = \frac{m+n}{1}$.

Proposition 14. *The multiplication* $\times : \begin{array}{ccc} \mathbb{Q} \times \mathbb{Q} & \to & \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) & \mapsto & \frac{ac}{bd} \end{array}$ *is well-defined.*

Proof. We need to prove that the multiplication doesn't depend on the choice of the representatives,
i.e. that if $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then $\frac{a}{b} \times \frac{c}{d} = \frac{a'}{b'} \times \frac{c'}{d'}$.
Assume that $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$, i.e. $ab' = ba'$ and $cd' = dc'$.
Therefore $(ac)(b'd') = ab'cd' = ba'dc' = (a'c')(bd)$, i.e. $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ as desired. ∎

Remark 15. Note that the multiplication defined on $\mathbb{Q}$ is compatible with the one on $\mathbb{Z}$.
Indeed, if $m, n \in \mathbb{Z}$ then $\frac{m}{1} \times \frac{n}{1} = \frac{m \times n}{1}$.

Definition 16. We define the binary relation $\leq$ on $\mathbb{Q}$ by

$$\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow 0 \leq (bc - ad)bd$$

where the order on the RHS of the equivalence is the order of $\mathbb{Z}$.

Remark 17. The idea behind the above definition is the following:
- We want that $\frac{a}{b} \leq \frac{c}{d}$ if and only if $0 \leq \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$, and,
- we also want that $0 \leq \frac{e}{f}$ if and only if $0 \leq ef$ (i.e. the sign rule).

Remark 18. We have to check that the order doesn't depend on the choice of representatives.

Remark 19. Note that the relation $\leq$ defined on $\mathbb{Q}$ is compatible with the usual order $\leq$ on $\mathbb{Z}$.
Indeed, let $m, n \in \mathbb{Z}$ then $\frac{m}{1} \leq \frac{n}{1} \Leftrightarrow 0 \leq n - m \Leftrightarrow m \leq n$.

Theorem 20. $(\mathbb{Q}, +, \times, \leq)$ *is a (totally) ordered field, meaning that*
- $+$ *is associative:* $\forall x, y, z \in \mathbb{Q}$, $(x + y) + z = x + (y + z)$
- 0 *is the unit of* $+$*:* $\forall x \in \mathbb{Q}$, $x + 0 = 0 + x = x$
- $-x$ *is the additive inverse of* x*:* $\forall x \in \mathbb{Q}$, $x + (-x) = (-x) + x = 0$
- $+$ *is commutative:* $\forall x, y \in \mathbb{Q}$, $x + y = y + x$
- $\times$ *is associative:* $\forall x, y, z \in \mathbb{Q}$, $(xy)z = x(yz)$
- $\times$ *is distributive with respect to* $+$*:* $\forall x, y, z \in \mathbb{Q}$, $x(y + z) = xy + xz$ *and* $(x + y)z = xz + yz$
- 1 *is the unit of* $\times$ *:* $\forall x \in \mathbb{Q}$, $1 \times x = x \times 1 = x$
- *If* $x \neq 0$ *then* x^{-1} *is the multiplicative inverse of* x*:* $\forall x \in \mathbb{Q} \setminus \{0\}$, $xx^{-1} = x^{-1}x = 1$
- $\times$ *is commutative:* $\forall x, y \in \mathbb{Q}$, $xy = yx$
- $\leq$ *is reflexive:* $\forall x \in \mathbb{Q}$, $x \leq x$

- $\leq$ *is antisymmetric:* $\forall x, y \in \mathbb{Q},\ \big(x \leq y \text{ and } y \leq x\big) \implies x = y$
- $\leq$ *is transitive:* $\forall x, y, z \in \mathbb{Q},\ \big(x \leq y \text{ and } y \leq z\big) \implies x \leq z$
- $\leq$ *is total:* $\forall x, y \in \mathbb{Q},\ x \leq y \text{ or } y \leq x$
- $\forall x, y, r, s \in \mathbb{Q},\ (x \leq y \text{ and } r \leq s) \Rightarrow x + r \leq y + s$
- $\forall x, y, z \in \mathbb{Q},\ \big(x \leq y \text{ and } z > 0\big) \Rightarrow xz \leq yz$

Remark 21. If $\frac{c}{d} \neq 0$, we set $\frac{\frac{a}{b}}{\frac{c}{d}} := \left(\frac{c}{d}\right)^{-1} \frac{a}{b} = \frac{ad}{bc}$.

Proposition 22. $\forall x, y \in \mathbb{Q},\ x < y \implies (\exists z \in \mathbb{Q},\ x < z < y)$

Proof. Let $x, y \in \mathbb{Q}$ be such that $x < y$. Then $z = \frac{x+y}{2}$ is a suitable choice.
Indeed, $x < y$ implies $2x < x + y$ and thus $x < z$. Similarly $x + y < 2y$, and thus $z < y$. ■

Theorem 23 ($\mathbb{Q}$ is archimedean)**.** $\forall \varepsilon \in \mathbb{Q}_{>0},\ \forall A \in \mathbb{Q}_{>0},\ \exists N \in \mathbb{N},\ N\varepsilon > A$.

Proof. Since $\frac{A}{\varepsilon} > 0$, we may find a representative $\frac{a}{b} = \frac{A}{\varepsilon}$ where $a, b \in \mathbb{N} \setminus \{0\}$.
Then $a + 1 - \frac{A}{\varepsilon} = a + 1 - \frac{a}{b} = \frac{a(b-1)+b}{b} > 0$, thus $(a + 1)\varepsilon > A$. So $N = a + 1$ is a suitable choice. ■

Remark 24. The above theorem means that $\lim\limits_{n \to +\infty} \frac{1}{n} = 0$, or equivalently that $\mathbb{Q}$ doesn't contain infinitesimal elements (i.e. there is not infinitely large or infinitely small elements).
This property may seem obvious at first glance, but, even if it is a little bit beyond the scope of this course, it is not too difficult to construct a (totally) ordered field with infinitesimal elements (i.e. with a positive element which is less than or equal to any other positive elements).

Remark 25. Note that $\mathbb{Q}$ is not well-ordered.
Indeed $\mathbb{Q}_{>0} = \{x \in \mathbb{Q} \ : \ x > 0\}$ is non-empty (and even bounded from below) but it has no least element.

Theorem 26 (The rational root theorem)**.**
Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ *be a polynomial with integer coefficients* $a_k \in \mathbb{Z}$.
If $x = \frac{p}{q}$ *is a rational root of* f *written in lowest terms* (*i.e.* $\gcd(p, q) = 1$)*, then* $p | a_0$ *and* $q | a_n$.

Proof. By assumption we have that

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \cdots + a_1 \frac{p}{q} + a_0 = 0$$

Therefore

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

Thus $p | a_0 q^n$. Since $\gcd(p, q) = 1$, by Gauss' lemma we obtain that $p | a_0$.
Similarly $q | a_n$. ■

3 Infima and suprema

Recall that a binary relation $\leq$ on a set E is an *order* if
(i) $\forall x \in E,\ x \leq x$ (*reflexivity*)
(ii) $\forall x, y \in E,\ \big(x \leq y \text{ and } y \leq x\big) \implies x = y$ (*antisymmetry*)
(iii) $\forall x, y, z \in E,\ \big(x \leq y \text{ and } y \leq z\big) \implies x \leq z$ (*transitivity*)

Definition 27. Let $(E, \leq)$ be an ordered set and $A \subset E$.
- We say that $m \in A$ is the *least element of* A if $\forall a \in A,\ m \leq a$.
- We say that $M \in A$ is the *greatest element of* A if $\forall a \in A,\ a \leq M$.

Remark 28. Note that, if it exists, the least element (resp. greatest element) of A is in A by definition.

Remark 29. The least (resp. greatest) element may not exist, but if it exists then it is unique.
For instance $\{n \in \mathbb{Z} \,:\, n \leq 0\} \subset \mathbb{Z}$ and $\{x \in \mathbb{Q} \,:\, 0 < x < 1\}$ have no least element.
For the uniqueness, it is easy to prove: assume that m, m' are two least elements of A, then

- $m \leq m'$ since m is *a* least element of A and $m' \in A$, and,
- $m' \leq m$ since m' is *a* least element of A and $m \in A$.

Hence $m = m'$.

Definition 30. Let $(E, \leq)$ be an ordered set and $A \subset E$.

- We say that A is *bounded from below* if it admits a *lower bound*, i.e.

$$\exists c \in E,\ \forall a \in A,\ c \leq a$$

- We say that A is *bounded from above* if it admits an *upper bound*, i.e.

$$\exists C \in E,\ \forall a \in A,\ a \leq C$$

- We say that A is *bounded* if it is bounded from below and from above.

Definition 31. Let $(E, \leq)$ be an ordered set and $A \subset E$.

- If the greatest lower bound of A exists, we denote it $\inf(A)$ and call it the *infimum of A*.
- If the least upper bound of A exists, we denote it $\sup(A)$ and call it the *supremum of A*.

Remark 32. If it exists, the greatest element of the set of lower bounds of A is unique (as shown above), therefore the infimum is unique (if it exists). And similarly for the supremum.
However, it may not exist:

- If $A = \{n \in \mathbb{Z} \,:\, n \leq 0\} \subset \mathbb{Z}$ then the set of lower bounds of A is empty, so A has no infimum.
- If $A = \left\{x \in \mathbb{Q} \,:\, x > 0 \text{ and } x^2 > 2\right\} \subset \mathbb{Q}$ then the set of lower bounds of A is not empty but has no greatest element, so A has no infimum.

Note that the infimum (resp. supremum) may not be an element of A, but if it is then it is the least (resp. greatest) element of A. For instance, the infimum of $A = \{x \in \mathbb{Q} \,:\, 0 < x < 1\} \subset \mathbb{Q}$ is $0 \notin A$.

4 Real numbers

The following results concerning $\mathbb{R}$ that you learnt during your first year calculus course are equivalent:

- The Least Upper Bound principle
- The Monotone Convergence Theorem for sequences
- The Extreme Value Theorem
- The Intermediate Value Theorem
- Rolle's Theorem/The Mean Value Theorem
- A continuous function on a segment line is Riemann-integrable
- *Bolzano-Weierstrass Property of* $\mathbb{R}$: a bounded sequence in $\mathbb{R}$ admits a convergent subsequence
- Cut property:

$$\forall A, B \subset \mathbb{R},\quad \left.\begin{array}{r} A, B \neq \varnothing \\ \mathbb{R} = A \cup B \\ \forall a \in A,\ \forall b \in B,\ a < b \end{array}\right\} \Longrightarrow \exists! c \in \mathbb{R},\ \forall a \in A,\ \forall b \in B,\ a \leq c \leq b$$

- ...

We say that $\mathbb{R}$ is Dedekind-complete to state that the above statements hold.

Intuitively, the Dedekind-completeness of the real line tells us two things:

1. There is no infinitely small positive real number (*Archimedean property*, which is already true for $\mathbb{Q}$):

$$\forall \varepsilon > 0,\ \forall A > 0,\ \exists n \in \mathbb{N},\ n\varepsilon > A$$

2. There is no gap in the real line. That's the difference with $\mathbb{Q}$. See for instance the following examples involving $\sqrt{2} \notin \mathbb{Q}$:
   - LUB: $\sqrt{2} = \sup\{x \in \mathbb{Q} \ : \ x^2 < 2\}$.
   - MCT: define a sequence by $x_0 = 1$ and $x_{n+1} = \frac{x_n}{2} + \frac{1}{x_n}$.
     Then (x_n) converges to some limit l by the MCT. But this limit must satisfy $l^2 = 2$.
   - IVT: let $f(x) = x^2 - 2$. Then $f(0) < 0$ and $f(2) > 0$.
     Hence we deduce from the IVT that f has a root, i.e. $\exists x \in \mathbb{R},\ x^2 - 2 = 0$.

The Dedekind-completeness of the real line has several consequences that you already know:
- The various results connecting the sign of f' to the monotonicity of f.
- $ACV \implies CV$ (for series and improper integrals).
- The Fundamental Theorem of Calculus.
- L'Hôpital's rule.
- The BCT and the LCT (for series and improper integrals).
- Cauchy-completeness of $\mathbb{R}$: any Cauchy sequence converges.
  Beware, despite very close names, without the Archimedean property Cauchy-completeness is strictly weaker than Dedekind-completeness.
- ⋯

Hence a first year calculus course is basically about the Dedekind-completeness of $\mathbb{R}$ and its consequences.

Theorem 33. *Up to isomorphism*[3]*, there exists a unique (totally) ordered field* $(\mathbb{R}, +, \times, \leq)$ *which is Dedekind-complete, i.e. such that:*
- $+$ *is associative:* $\forall x, y, z \in \mathbb{R},\ (x + y) + z = x + (y + z)$
- 0 *is the unit of* $+$*:* $\forall x \in \mathbb{R},\ x + 0 = 0 + x = x$
- *Existence of the additive inverse:* $\forall x \in \mathbb{R},\ \exists(-x) \in \mathbb{R},\ x + (-x) = (-x) + x = 0$
- $+$ *is commutative:* $\forall x, y \in \mathbb{R},\ x + y = y + x$
- $\times$ *is associative:* $\forall x, y, z \in \mathbb{R},\ (xy)z = x(yz)$
- $\times$ *is distributive with respect to* $+$*:* $\forall x, y, z \in \mathbb{R},\ x(y + z) = xy + xz$ *and* $(x + y)z = xz + yz$
- 1 *is the unit of* $\times$*:* $\forall x \in \mathbb{R},\ 1 \times x = x \times 1 = x$
- *Existence of the multiplicative inverse:* $\forall x \in \mathbb{R} \setminus \{0\},\ \exists x^{-1} \in \mathbb{R},\ xx^{-1} = x^{-1}x = 1$
- $\times$ *is commutative:* $\forall x, y \in \mathbb{R},\ xy = yx$
- $\leq$ *is reflexive:* $\forall x \in \mathbb{R},\ x \leq x$
- $\leq$ *is antisymmetric:* $\forall x, y \in \mathbb{R},\ \big(x \leq y \text{ and } y \leq x\big) \implies x = y$
- $\leq$ *is transitive:* $\forall x, y, z \in \mathbb{R},\ \big(x \leq y \text{ and } y \leq z\big) \implies x \leq z$
- $\leq$ *is total:* $\forall x, y \in \mathbb{R},\ x \leq y$ *or* $y \leq x$
- $\forall x, y, r, s \in \mathbb{R},\ (x \leq y \text{ and } r \leq s) \Rightarrow x + r \leq y + s$
- $\forall x, y, z \in \mathbb{R},\ \big(x \leq y \text{ and } z > 0\big) \Rightarrow xz \leq yz$
- $\mathbb{R}$ *is Dedekind-complete (for instance a non-empty subset which is bounded from above admits a supremum).*

The theorem contains two parts: existence and uniqueness.

For the existence part, there are several ways to construct a field satisfying the above properties. Usually each construction gives easily a version of the Dedekind-completeness from which we derive the other equivalent statements.

One very common construction consists in defining $\mathbb{R}$ as equivalence classes of rational Cauchy sequences: this way we obtain easily the archimedean property and the Cauchy-completeness (which are together equivalent to the Dedekind-completeness).

Another common construction relies on Dedekind cuts (that I present in the appendix). This one gives the cut property for free, from which we easily derive the least upper bound principle (quite often the LUB

[3] It means that if we have two such fields, then there is a bijection between them preserving the addition, the multiplication and the order, i.e. they are basically the same.

principle is the start point of first year calculus courses).

The uniqueness part is a little bit delicate and I won't prove it in this course. Nonetheless, let me try to explain the rough idea.

Assume that we are given two fields $\mathbb{R}$ and $\tilde{\mathbb{R}}$ satisfying the above properties. Note that each of them contains a copy of $\mathbb{Q}$. Then we can construct a order-preserving bijection $\varphi : \mathbb{R} \to \tilde{\mathbb{R}}$ compatible with the addition and the multiplication as follows: first we map the copy of $\mathbb{Q}$ in $\mathbb{R}$ to the one in $\tilde{\mathbb{R}}$ and then we use the Dedekind-completeness to extend the bijection from $\mathbb{Q}$ to $\mathbb{R}$ (the idea is to *fill the gaps* similarly in $\mathbb{R}$ and $\tilde{\mathbb{R}}$).

Nonetheless, there is no need to give an explicit construction of $\mathbb{R}$: we can use the above properties as axioms and then study their consequences. That's the usual strategy in a first year calculus course. In the sequel, concerning the Dedekind-completeness of $\mathbb{R}$, we assume that the least upper bound principle holds:

LUB Principle. A non-empty subset of $\mathbb{R}$ which is bounded from above admits a supremum.

Proposition 34. *$\mathbb{Q} \subset \mathbb{R}$ and $+, \times, <$ for $\mathbb{R}$ are compatible with the ones for $\mathbb{Q}$.*

Proof. That's a sketch of proof (for concision I use equality instead of identification/bijection).

1. $\mathbb{N} \subset \mathbb{R}$: if $n \in \mathbb{N}$ then $n = 1 + 1 + \cdots + 1 \in \mathbb{R}$. So $\mathbb{N} \subset \mathbb{R}$.
2. $\mathbb{Z} \subset \mathbb{R}$: if $n \in \mathbb{N}$ then $-n \in \mathbb{R}$. So $\mathbb{Z} \subset \mathbb{R}$.
3. $\mathbb{Q} \subset \mathbb{R}$: if $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ then $\frac{a}{b} \coloneqq ab^{-1} \in \mathbb{R}$. So $\mathbb{Q} \subset \mathbb{R}$.

■

Proposition 35.

- $\forall x, y, z \in \mathbb{R},\ x \leq y \Rightarrow x + z \leq y + z$
- $\forall x, y, z \in \mathbb{R},\ (x \leq y \text{ and } 0 \leq z) \Rightarrow xz \leq yz$
- $\forall x, y, u, v \in \mathbb{R},\ (x \leq y \text{ and } u \leq v) \Rightarrow x + u \leq y + v$
- $\forall x \in \mathbb{R},\ 0 < x \Leftrightarrow 0 < \frac{1}{x}$
- $\forall x, y \in \mathbb{R},\ \forall z \in \mathbb{R}_+^*,\ x \leq y \Leftrightarrow xz \leq yz$
- $\forall x, y, u, v \in \mathbb{R},\ (0 \leq x \leq y \text{ and } 0 \leq u \leq v) \Rightarrow xu \leq yv$
- $\forall x, y \in \mathbb{R},\ 0 < x < y \Leftrightarrow \frac{1}{y} < \frac{1}{x}$

Definition 36. We define the *absolue value* by $|\cdot| : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & |x| \end{array}$ $\coloneqq \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x \leq 0 \end{cases}$

Proposition 37.

- $\forall x \in \mathbb{R},\ |x| = \max(x, -x)$
- $\forall x \in \mathbb{R},\ |x| \geq 0$
- $\forall x \in \mathbb{R},\ x = 0 \Leftrightarrow |x| = 0$
- $\forall x, y \in \mathbb{R},\ |x| = |y| \Leftrightarrow (x = y \text{ or } x = -y)$
- $\forall x, y \in \mathbb{R},\ |xy| = |x||y|$
- $\forall x \in \mathbb{R} \setminus \{0\},\ \left|\frac{1}{x}\right| = \frac{1}{|x|}$
- $\forall x, y \in \mathbb{R},\ |x + y| \leq |x| + |y|$ (*triangle inequality*)
- $\forall x, y \in \mathbb{R},\ ||x| - |y|| \leq |x - y|$ (*reverse triangle inequality*)

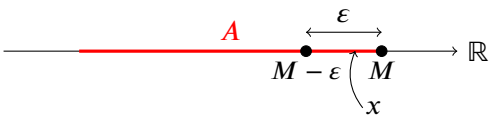
Proposition 38. *For $x, a \in \mathbb{R}$,*

- $|x| \leq a \Leftrightarrow -a \leq x \leq a$
- $|x| < a \Leftrightarrow -a < x < a$
- $|x| \geq a \Leftrightarrow (x \geq a \text{ or } x \leq -a)$
- $|x| > a \Leftrightarrow (x > a \text{ or } x < -a)$
- *If $a \geq 0$ then* $|x| = a \Leftrightarrow (x = a \text{ or } x = -a)$

Proposition 39. *Let $A \subset \mathbb{R}$ and $M \in \mathbb{R}$. Then*

$$M = \sup(A) \Leftrightarrow \begin{cases} \forall x \in A,\ x \leq M \\ \forall \varepsilon > 0,\ \exists x \in A,\ M - \varepsilon < x \end{cases}$$

The first condition ensures that M is an upper bound of A. The second one means it is the smallest one.



Beware, for simplicity I represented A as an interval in the above figure, but it may not be an interval!

Proof.
$\Rightarrow$ Assume that $M = \sup(A)$. Then M is an upper bound of A so $\forall x \in A,\ x \leq S$.
We know that if T is an other upper bound of A then $M \leq T$ (since M is the least upper bound).
So, by taking the contrapositive, if $T < M$ then T isn't an upper bound of A.
Let $\varepsilon > 0$. Since $M - \varepsilon < M$, we know that $M - \varepsilon$ is not an upper bound of A, meaning that there exists $x \in A$ such that $M - \varepsilon < x$.

$\Leftarrow$ Assume that

$$\begin{cases} \forall x \in A,\ x \leq M \\ \forall \varepsilon > 0,\ \exists x \in A,\ M - \varepsilon < x \end{cases}$$

Then, by the first condition, M is an upper bound of A. Let's prove it is the least one.
We will show the contrapositive: if $T < M$ then T isn't an upper bound of A.
Let $T \in \mathbb{R}$. Assume that $T < M$. Set $\varepsilon = M - T > 0$. Then there exists $x \in A$ such that $M - \varepsilon < x$, i.e. $T < x$.
Hence T isn't an upper bound of A ■

We have a similar characterization for the infimum.

Proposition 40. *Let $A \subset \mathbb{R}$ and $m \in \mathbb{R}$. Then*

$$m = \inf(A) \Leftrightarrow \begin{cases} \forall x \in A,\ m \leq x \\ \forall \varepsilon > 0,\ \exists x \in A,\ x < m + \varepsilon \end{cases}$$

Proposition 41. *Given $A, B \subset \mathbb{R}$ two non-empty subsets of $\mathbb{R}$, we set*
- $A + B = \{x \in \mathbb{R} \ :\ \exists a \in A,\ \exists b \in B,\ x = a + b\}$
- $-A = \{x \in \mathbb{R} \ :\ -x \in A\}$

Then
- *If A and B are bounded from above then $A + B$ is too and* $\sup(A + B) = \sup(A) + \sup(B)$.
- *If A is bounded from above then $-A$ is bounded from below and* $\inf(-A) = -\sup(A)$.
- *If A and B are bounded from above then $A \cup B$ is too and* $\sup(A \cup B) = \max(\sup(A), \sup(B))$

Theorem 42 ($\mathbb{R}$ is archimedean)**.** $\forall \varepsilon > 0,\ \forall A > 0,\ \exists n \in \mathbb{N},\ n\varepsilon > A$

Proof. Let $\varepsilon > 0$ and $A > 0$.
Assume by contradiction that $\forall n \in \mathbb{N},\ n\varepsilon \leq A$. Then $E = \{n\varepsilon \ :\ n \in \mathbb{N}\}$ is non-empty and bounded from above so it admits a supremum $M = \sup E$ by the least upper bound principle.
Since $M - \varepsilon < M$, $M - \varepsilon$ is not an upper bound of E, so there exists $n \in \mathbb{N}$ such that $n\varepsilon > M - \varepsilon$.
Therefore $(n + 1)\varepsilon > M$, hence a contradiction. ■

Proposition 43. *For every $x \in \mathbb{R}$, there exists a unique $n \in \mathbb{Z}$ such that $n \leq x < n + 1$.*
We say that n is the integer part (or the floor function value) of x and we denote it by $\lfloor x \rfloor$.

Proof. Let $x \in \mathbb{R}$.
Existence.
- *First case: if* $x \geq 0$.
  We set $E = \{n \in \mathbb{N} \ : \ x < n\}$.
  By the archimedean property (with $\varepsilon = 1$), there exists $m \in \mathbb{N}$ such that $m > x$. Hence $E \neq \varnothing$.
  By the well-ordering principle, E admits a least element p.
  We have that $x < p$ since $p \in E$ and that $p - 1 \leq x$ since $p - 1 \notin E$.
  Therefore $n = p - 1$ satisfies $n \leq x < n + 1$.
- *Second case: if* $x < 0$. Then we apply the first case to $-x$.

Uniqueness. Assume that $n, n' \in \mathbb{Z}$ are two suitable integers, then

$$n \leq x < n + 1 \tag{1}$$

and

$$n' \leq x < n' + 1$$

We deduce from the last inequality that

$$-n' - 1 < -x \leq -n' \tag{2}$$

Summing (1) and (2), we get that $n - n' - 1 < 0 < n - n' + 1$.
Hence $n - n' < 1$, i.e. $n - n' \leq 0$, and $-1 < n - n'$ i.e. $0 \leq n - n'$.
Therefore $n = n'$. ∎

Remark 44. We have $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$, from which we derive $x - 1 < \lfloor x \rfloor \leq x$.

Theorem 45 ($\mathbb{Q}$ is dense in $\mathbb{R}$)**.** $\forall x, y \in \mathbb{R},\ x < y \Rightarrow (\exists q \in \mathbb{Q},\ x < q < y)$

Proof. Let $x, y \in \mathbb{R}$ be such that $x < y$. Set $\varepsilon = y - x > 0$.
By the archimedean property, there exists $n \in \mathbb{N} \setminus \{0\}$ such that $n\varepsilon > 1$, i.e. $\frac{1}{n} < \varepsilon$.
Set $m = \lfloor nx \rfloor + 1$. Then $nx < m \leq nx + 1$, so $x < \frac{m}{n} \leq x + \frac{1}{n} < x + \varepsilon = y$. ∎

Remark 46. The above theorem is equivalent to the fact that any real number is the limit of a sequence of rational numbers (that you will prove in Problem Set).

Definition 47. A subset $I \subset \mathbb{R}$ is an *interval* if $\forall x, y \in I$, $\forall z \in \mathbb{R}$, $(x \leq z \leq y \Rightarrow z \in I)$.

Proposition 48. *If $I \subset \mathbb{R}$ is a non-empty interval not reduced to a singleton then $I \cap \mathbb{Q} \neq \varnothing$.*

Proof. Since I is non-empty and not reduced to a singleton, there exist $x, y \in I$ with $x < y$.
Then, since $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists $q \in \mathbb{Q}$ such that $x < q < y$.
Since I is an interval, $q \in I$. Hence $q \in I \cap \mathbb{Q} \neq \varnothing$. ∎

Corollary 49. $\forall x, y \in \mathbb{R},\ x < y \implies (\exists s \in \mathbb{R} \setminus \mathbb{Q},\ x < s < y)$

Proof. Let $x, y \in \mathbb{R}$ be such that $x < y$.
By Theorem 45, there exists $q \in \mathbb{Q}$ such that $x < q < y$.
Still by Theorem 45, there exists $p \in \mathbb{Q}$ such that $x < p < q$.
Hence we obtained $p, q \in \mathbb{Q}$ such that $x < p < q < y$.
Set $s = p + \frac{\sqrt{2}}{2}(q - p)$. Then $s \in \mathbb{R} \setminus \mathbb{Q}$ (otherwise, by contradiction, $\sqrt{2}$ would be in $\mathbb{Q}$, which is not the case as you proved in the Week 4 of tutorials) and $p < s < q$ (notice that $0 < \frac{\sqrt{2}}{2} < 1$ so s is a number between p and q).
We obtained $s \in \mathbb{R} \setminus \mathbb{Q}$ such that $x < s < y$. ∎

Proposition 50. *If $I \subset \mathbb{R}$ is an interval which is non-empty and not reduced to a singleton then $I \cap (\mathbb{R} \setminus \mathbb{Q}) \neq \varnothing$.*

5 Decimal representation of real numbers

It is possible to generalize the decimal numeral system used to describe integers in order to describe real numbers. In what follows I only work with decimal expansions but all the statements/proofs work if we replace 10 by $b \geq 2$.

We start with a lemma that we will use several times in this section.

Lemma 51. *Let $(a_k)_{k\geq 1}$ be a sequence such that $\forall k \in \mathbb{N}\setminus\{0\}$, $a_k \in \{0,1,\dots,9\}$. Then the series*

$$S = \sum_{k=1}^{+\infty} \frac{a_k}{10^k}$$

is convergent and $S \geq 0$.

Proof.

Note that $0 \leq \dfrac{a_k}{10^k} \leq \dfrac{9}{10^k}$ and that $\displaystyle\sum_{k=1}^{+\infty} \frac{9}{10^k}$ is convergent (geometric series with ratio $\dfrac{1}{10} < 1$).
Therefore we may conclude using the BCT. ■

Remark 52. Unfortunately the decimal representation may not be unique:

$$0.9999\dots = \sum_{k=1}^{+\infty} \frac{9}{10^k} = \frac{9}{10} \times \frac{1}{1-\frac{1}{10}} = 1.000\dots$$

In order to achieve uniqueness we are going to restrict to expansions which don't end with infinitely many 9, see the definition below.

Definition 53. Let $x \in \mathbb{R}$. We say that

$$\lfloor x \rfloor + \sum_{k=1}^{+\infty} \frac{a_k}{10^k}$$

is a *proper decimal expansion of x* if

(i) $\forall k \in \mathbb{N}\setminus\{0\}$, $a_k \in \{0,1,\dots,9\}$

(ii) $\forall n \in \mathbb{N}\setminus\{0\}$, $\displaystyle\sum_{k=1}^{n} \frac{a_k}{10^k} \leq x - \lfloor x \rfloor < \sum_{k=1}^{n} \frac{a_k}{10^k} + \frac{1}{10^n}$

Proposition 54. *If $\lfloor x \rfloor + \displaystyle\sum_{k=1}^{+\infty} \frac{a_k}{10^k}$ is a proper decimal expansion of $x \in \mathbb{R}$ then*

1. $x = \lfloor x \rfloor + \displaystyle\sum_{k=1}^{+\infty} \frac{a_k}{10^k}$
2. $\forall N \in \mathbb{N}\setminus\{0\}$, $\exists k > N$, $a_k \neq 9$

Then we simply write $x = \lfloor x \rfloor . a_1 a_2 a_3 \dots$.

Remark 55. The last item means that a proper decimal expansion can't end with infinitely many 9.

Proof.

1. We already proved that $S = \displaystyle\sum_{k=1}^{+\infty} \frac{a_k}{10^k}$ is convergent. Hence we get $S \leq x - \lfloor x \rfloor \leq S$. So $x = \lfloor x \rfloor + S$.

2. Assume by contradiction that there exists $N \in \mathbb{N} \setminus \{0\}$ such that $\forall k > N$, $a_k = 9$.
   Then $x - \lfloor x \rfloor = \sum_{k=1}^{+\infty} \frac{a_k}{10^k} = \sum_{k=1}^{N} \frac{a_k}{10^k} + \sum_{k=N+1}^{+\infty} \frac{9}{10^k} = \sum_{k=1}^{N} \frac{a_k}{10^k} + \frac{1}{10^N}$. Which contradicts the definition of proper decimal expansion (the strict inequality in 53.(ii)).

■

Theorem 56. *A real number x admits a unique proper decimal expansion.*

Proof. Let $x \in \mathbb{R}$. Up to replacing x with $x - \lfloor x \rfloor$, we may assume that $\lfloor x \rfloor = 0$.
Assume that $\sum_{k=1}^{+\infty} \frac{a_k}{10^k}$ is a proper decimal expansion of x.
Then, from 53.(ii), we get that

$$a_n \leq 10^n \left(x - \sum_{k=1}^{n-1} \frac{a_k}{10^k} \right) < a_n + 1$$

So the only possible suitable sequence (a_n) is given by $a_1 = \lfloor 10x \rfloor$ and $a_{n+1} = \left\lfloor 10^{n+1} \left(x - \sum_{k=1}^{n} \frac{a_k}{10^k} \right) \right\rfloor$.
It proves the uniqueness, but we still need to check that it is valid.

(i) Since $\lfloor x \rfloor = 0$, we have $0 \leq x < 1$. Thus $0 \leq 10x < 10$. Therefore $a_1 = \lfloor 10x \rfloor \in \{0, 1, \dots, 9\}$.
Let $n \in \mathbb{N} \setminus \{0\}$, then

$$0 \leq 10^n \left(x - \sum_{k=1}^{n-1} \frac{a_k}{10^k} \right) - a_n < 1$$

Thus

$$0 \leq 10^{n+1} \left(x - \sum_{k=1}^{n} \frac{a_k}{10^k} \right) < 10$$

Therefore $a_{n+1} \in \{0, 1, \dots, 9\}$.

(ii) We have $\forall n \in \mathbb{N} \setminus \{0\}$, $\sum_{k=1}^{n} \frac{a_k}{10^k} \leq x < \sum_{k=1}^{n} \frac{a_k}{10^k} + \frac{1}{10^n}$ by construction.

■

Remark 57. It is easy to compute the decimal expansion of a rational number.
Indeed, let $x = \frac{a}{b}$ where $a \in \mathbb{Z}$ and $b \in \mathbb{N} \setminus \{0\}$.
By Euclidean division, $a = bq_0 + r_0$ where $0 \leq r_0 < b$. Hence $\frac{a}{b} = q_0 + \frac{r_0}{b}$. Note that $q_0 = \left\lfloor \frac{a}{b} \right\rfloor$.
Now, again by Euclidean division, $10r_0 = bq_1 + r_1$ where $0 \leq r_1 < b$.
And we repeat: $10r_k = bq_{k+1} + r_{k+1}$ where $0 \leq r_{k+1} < b$.
According to the *pigeonhole principle* (or the *Dirichlet's drawer principle*), since there are only b possible remainders, the process will start looping after at most b steps.
But note that the $(q_k)_{k \geq 1}$ defines exactly the decimal expansion of x.
Therefore the decimal expansion of a rational is eventually periodic.

Definition 58. We say that a proper decimal expansion is eventually periodic if

$$\exists r \in \mathbb{N},\ \exists s \in \mathbb{N} \setminus \{0\},\ \forall k \in \mathbb{N},\ a_{r+k+s} = a_{r+k}$$

It means that

$$\begin{aligned} x &= \lfloor x \rfloor . b_1 b_2 \dots b_r \underline{c_1 c_2 \dots c_s} \\ &:= \lfloor x \rfloor . b_1 b_2 \dots b_r c_1 c_2 \dots c_s c_1 c_2 \dots c_s c_1 \dots \end{aligned}$$

Example 59. We want to find the decimal expansion of $\frac{1529327}{24975}$.

1. $1529327 = 24975 \times 61 + 5852$
2. $58520 = 24975 \times 2 + 8570$
3. $85700 = 24975 \times 3 + 10775$
4. $107750 = 24975 \times 4 + 7850$
5. $78500 = 24975 \times 3 + 3575$
6. $35750 = 24975 \times 1 + 10775$

And we start to loop. Therefore $\frac{1529327}{24975} = 61.234\underline{314}$

Theorem 60. *A real number x is rational if and only if its proper decimal expansion is eventually periodic.*

Proof.
$\Rightarrow$ That's exactly Remark 57.

$\Leftarrow$ Assume that the proper decimal expansion $x = \lfloor x \rfloor + \sum_{k=1}^{+\infty} \frac{a_k}{10^k}$ is eventually periodic,

i.e. $\exists r \in \mathbb{N}$, $\exists s \in \mathbb{N} \setminus \{0\}$, $\forall k \in \mathbb{N}$, $a_{r+k+s} = a_{r+k}$.

Then $x = \lfloor x \rfloor + \sum_{k=1}^{r} \frac{a_k}{10^k} + 10^{-r} \sum_{k=1}^{+\infty} \frac{a_{r+k}}{10^k}$.

Hence it is enough to prove that $y = \sum_{k=1}^{+\infty} \frac{a_{r+k}}{10^k} \in \mathbb{Q}$.

Note that $10^s y = N + y$ where $N = \overline{a_{r+1}a_{r+2}\dots a_{r+s}}^{10} \in \mathbb{N}$. Hence $y = \frac{N}{10^s - 1} \in \mathbb{Q}$. ∎

Remark 61. According to the above proof,

$$\begin{aligned} a_t a_{t-1} \dots a_0 . b_1 b_2 \dots b_r \underline{c_1 c_2 \dots c_s} &= \overline{a_t a_{t-1} \cdots a_0}^{10} + \sum_{k=1}^{r} \frac{b_k}{10^k} + 10^{-r} \frac{\overline{c_1 c_2 \dots c_s}^{10}}{10^s - 1} \\ &= \overline{a_t a_{t-1} \dots a_0}^{10} + \frac{\overline{b_1 b_2 \dots b_r}^{10}}{10^r} + \frac{\overline{c_1 c_2 \dots c_s}^{10}}{10^{r+s} - 10^r} \\ &= \frac{\overline{a_t a_{t-1} \dots a_0 b_1 b_2 \dots b_r c_1 c_2 \dots c_s}^{10} - \overline{a_t a_{t-1} \dots a_0 b_1 b_2 \dots b_r}^{10}}{10^{r+s} - 10^r} \end{aligned}$$

Example 62.

- $61.234\underline{314} = \frac{61234314 - 61234}{10^6 - 10^3} = \frac{61173080}{999000}$
- $0.\underline{3} = \frac{3 - 0}{10 - 1} = \frac{3}{9}$
- $42.\underline{012} = \frac{42012 - 42}{10^3 - 1} = \frac{41970}{999}$

6 $\sqrt{2}$ is irrational

Using the IVT, we may prove that there exists a unique positive real number $x > 0$ such that $x^2 = 2$.
We denote it by $\sqrt{2}$.

Theorem 63. $\sqrt{2} \notin \mathbb{Q}$

Below are some of my favorite proofs for the irrationality of $\sqrt{2}$.

Proof 1 (Fundamental Theorem of Arithmetic).
Assume by contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$. Then $2b^2 = a^2$.
The prime factorization of the LHS has an odd number of primes (counted with exponents) whereas the RHS has an even number of primes (counted with exponents).
Which is impossible since the prime factorization is unique up to order. ∎

Proof 2 (*Euclid's lemma*).
Assume by contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ written in lowest form.
Then $2b^2 = a^2$. Therefore $2|a^2$. By Euclid's lemma, $2|a$, so $a = 2k$.
Thus $2b^2 = 4k^2$, from which we get $b^2 = 2k^2$. By Euclid's lemma, $2|b$.
Hence $2|\gcd(a, b) = 1$, which is a contradiction. ■

Proof 3 (*Gauss' lemma*).
Assume by contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ written in lowest form.
Then $2b^2 = a^2$. Therefore $b|a^2$.
Since $\gcd(a, b) = 1$, by Gauss' lemma (applied twice), $b|1$ and hence $b = 1$ (since $b \in \mathbb{N} \setminus \{0\}$ in lowest form).
Hence $a^2 = 2$. Which is impossible (2 is not a perfect square: $\forall x \in \mathbb{Z}$, $x^2 \equiv 0 \pmod 3$ or $x^2 \equiv 1 \pmod 3$). ■

Proof 4 (*proof by infinite descent*).
Assume by contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ where $a \in \mathbb{N}$ and $b \in \mathbb{N} \setminus \{0\}$.
Then $2b^2 = a^2$. Then $a(a - b) = a^2 - ab = 2b^2 - ab = b(2b - a)$. Hence $\sqrt{2} = \frac{a}{b} = \frac{2b-a}{a-b}$.
Note that $1 < \sqrt{2} = \frac{a}{b}$, thus $0 < a - b$. Therefore $0 < 2b - a$, so $a - b < b$.
Therefore we obtained another expression of $\sqrt{2}$ with a smaller positive denominator.
By repeating this process, we may construct an infinite sequence $\sqrt{2} = \frac{a}{b} = \frac{a_1}{b_1} = \frac{a_2}{b_2} = \cdots$ such that $a_k > 0$ and $0 < b_{k+1} < b_k$.
Which is a contradiction since there is no decreasing infinite sequence of natural numbers. ■

Proof 5 (*by congruences*).
Assume by contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ written in lowest form. Then $2b^2 = a^2$.
Since $\gcd(a, b) = 1$, we can't have $a \equiv 0 \pmod 3$ and $b \equiv 0 \pmod 3$ simulatenously (otherwise $3|\gcd(a, b)$).

- Either $a \equiv \pm 1 \pmod 3$ and $b \equiv 0 \pmod 3$, then $a^2 - 2b^2 \equiv 1 \pmod 3$,
- or $a \equiv 0 \pmod 3$ and $b \equiv \pm 1 \pmod 3$, then $a^2 - 2b^2 \equiv 1 \pmod 3$,
- or $a \equiv \pm 1 \pmod 3$ and $b \equiv \pm 1 \pmod 3$, then $a^2 - 2b^2 \equiv 2 \pmod 3$.

Therefore $a^2 - 2b^2 \not\equiv 0 \pmod 3$ and so $a^2 - 2b^2 \neq 0$. Which is a contradiction. ■

Proof 6 (*by the well-ordering principle*).
Assume by contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$. Then $a = \sqrt{2}b$.
Therefore $E = \left\{ n \in \mathbb{N} \ : \ n\sqrt{2} \in \mathbb{N} \setminus \{0\} \right\}$ is not empty since it contains $|b|$ as $\sqrt{2}|b| = |a|$.
By the well-ordering principle, E admits a least element p. Then $p\sqrt{2} \in \mathbb{N} \setminus \{0\}$.
Set $q = p\sqrt{2} - p$. Then $q \in \mathbb{Z}$. Besides $q = p(\sqrt{2} - 1)$ so that $0 < q < p$.
But $q\sqrt{2} = 2p - p\sqrt{2} = p - q \in \mathbb{N} \setminus \{0\}$. So $q \in E$.
Which is a contradiction since p is the least element of E and $q < p$. ■

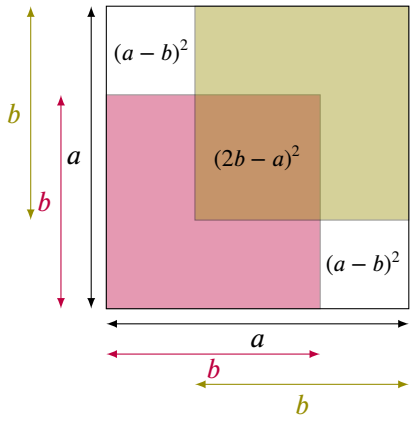
Proof 7 (*by the rational root theorem*).
Assume by contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ written in lowest form.
Since $\sqrt{2} = \frac{a}{b}$ is a root of $x^2 - 2 = 0$, we deduce from the rational root theorem that $a|2$ and $b|1$.
So either $\sqrt{2} = \pm 1$ or $\sqrt{2} = \pm 2$.
We obtain a contradiction in both cases since $(\pm 1)^2 = 1 \neq 2$ and $(\pm 2)^2 = 4 \neq 2$. ■

Proof 8 (*by the archimedean property*).
For $n \in \mathbb{N}$, set $u_n = \left(\sqrt{2}-1\right)^n$. We may prove either by induction or using the binomial formula, that for every n, there exist $a_n, b_n \in \mathbb{Z}$ such that $u_n = a_n + b_n\sqrt{2}$.
Since[4] $0 < \sqrt{2}-1 < \frac{1}{2}$, we may also prove that $0 < u_n \leq \frac{1}{2^n}$.
Assume by contradiction that $\sqrt{2} = \frac{p}{q} \in \mathbb{Q}$, then

$$u_n = a_n + b_n\sqrt{2} = a_n + b_n\frac{p}{q} = \frac{qa_n + pb_n}{q}$$

Since $u_n > 0$ we get that $|qa_n + pb_n| \geq 1$ and that $u_n \geq \frac{1}{|q|}$.
Therefore $\forall n \in \mathbb{N}$, $0 < \frac{1}{|q|} \leq u_n \leq \frac{1}{2^n}$. Which contradicts the archimedean property. ■

Proof 9 (*geometric version of proof 4*).
Assume by contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ where $a \in \mathbb{N}$ and $b \in \mathbb{N} \setminus \{0\}$. Then $a = \sqrt{2}b > b$.

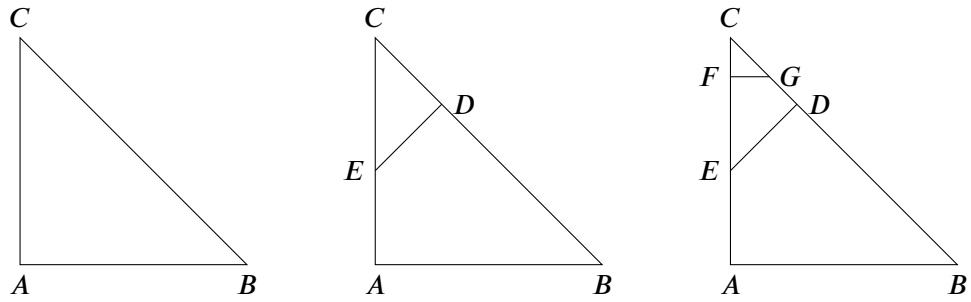


By a direct computation of the side length, the square at the center has an area of $\mathcal{A} = (2b-a)^2$.
But, by inclusion-exclusion, $\mathcal{A}$ also satisfies $2(a-b)^2 + 2b^2 - \mathcal{A} = a^2$.
So $\mathcal{A} = 2(a-b)^2 + 2b^2 - a^2 = 2(a-b)^2$ since $a^2 = 2b^2$.
Therefore $2(a-b)^2 = \mathcal{A} = (2b-a)^2$. Thus $2 = \frac{(2b-a)^2}{(a-b)^2}$.
Hence $\sqrt{2} = \frac{2b-a}{a-b}$ with[5] $0 < 2b-a$ and $0 < a-b < b$.
By repeating this process, we may construct an infinite sequence $\sqrt{2} = \frac{a}{b} = \frac{a_1}{b_1} = \frac{a_2}{b_2} = \cdots$ such that $a_k > 0$ and $0 < b_{k+1} < b_k$.
Which is a contradiction since there is no decreasing infinite sequence of natural numbers. ■

Proof 10 (*Pythagoras flavored*).
Let ABC be a isosceles right triangle in A. By the Pythagorean theorem $\frac{\overline{BC}}{\overline{AB}} = \sqrt{2}$.
Assuming that $\sqrt{2}$ is rational means geometrically that $\overline{BC}$ and $\overline{AB}$ are commensurable, i.e. they are both integral multiple of a another length d[6].
Put D on $[BC]$ such that $\overline{BD} = \overline{AB}$.
Define E as the intersection of (AC) with the line through D which is perpendicular to (BC).

[4] Use the fact that $(0,+\infty) \ni x \to x^2 \in \mathbb{R}$ is increasing and that $2 \leq \left(\frac{3}{2}\right)^2$ to conclude that $\sqrt{2} \leq \frac{3}{2}$.
[5] See Proof 4 for $0 < 2b-a$.
[6] That is the geometric version of *irrationality* used by ancient Greeks:
if $\sqrt{2} = \frac{a}{b}$, set $d = \frac{\overline{AB}}{b}$ then $\overline{AB} = bd$ and $\overline{BC} = \sqrt{2} \times \overline{AB} = \frac{a}{b}bd = ad$.

Note that[7] $\overline{AE} = \overline{ED} = \overline{DC}$.
Thus $\overline{CD} = \overline{BC} - \overline{AB}$ and $\overline{EC} = \overline{AC} - \overline{AE} = \overline{AB} - (\overline{BC} - \overline{AB}) = 2\overline{AB} - \overline{BC}$.
Therefore $\overline{CD}$ and $\overline{EC}$ are integral multiple of d.
Besides DEC is a isosceles right triangle in D, therefore we may repeat this construction on the triangle DEC in order to construct an infinite sequence of segment lines ($AC, EC, FC, \ldots$, see below) which are all integral multiple of d and with decreasing length.
Which is impossible.



■

The above proof is actually another geometric version of Proof 4:

Algebraically: $\dfrac{2b-a}{a-b} = \dfrac{2-a/b}{a/b-1} = \dfrac{2-\sqrt{2}}{\sqrt{2}-1} = \sqrt{2}$.

Geometrically: $\sqrt{2} = \dfrac{\overline{EC}}{\overline{CD}} = \dfrac{2\overline{AB} - \overline{BC}}{\overline{BC} - \overline{AB}}$.

Proof 11 (*my favorite one*).
The proof is left as an exercise to the reader. ■

Before leaving $\sqrt{2}$, I would like to show you a funny proof relying on the *tertium non datur*.

Proposition 64. *There exist $a, b > 0$ irrational numbers such that $a^b \in \mathbb{Q}$.*

Proof.

- Assume that $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$. Then we can take $a = b = \sqrt{2}$.
- Assume that $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$. Then we can take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. Indeed, $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$.

■

Remark 65. Note that in the above proof it is not necessary to know whether $\sqrt{2}^{\sqrt{2}}$ is rational or not in order to conclude! That's really cool! By the way, it is not rational using Gelfond–Schneider Theorem.

[7] Compare the triangles BAE and BDE which are respectively right in A and D with common hypotenuse and $\overline{AB} = \overline{DB}$, so, by the Pythagorean theorem, $\overline{AE} = \overline{ED}$. Besides the triangle CDE is isosceles right in A by angle considerations, thus $\overline{ED} = \overline{DC}$.

7 e is irrational

You know from your first year calculus that $e = \sum_{n=0}^{+\infty} \frac{1}{n!}$.

Theorem 66. $e \notin \mathbb{Q}$

Proof 1. Assume by contradiction that $e = \frac{a}{b}$ where $a, b \in \mathbb{N} \setminus \{0\}$. Note that $b > 1$ since $e \notin \mathbb{N}$. Besides

$$b!\left(e - \sum_{n=0}^{b} \frac{1}{n!}\right) = b!\left(\sum_{n\geq b+1} \frac{1}{n!}\right)$$

Note that the LHS is an integer. We are going to derive a contradiction by proving that the RHS is not an integer. Indeed

$$0 < b!\left(\sum_{n\geq b+1} \frac{1}{n!}\right) \leq \sum_{n\geq 1} \frac{1}{(b+1)^n} = \frac{1}{b} < 1$$

■

It is also possible to use an approach similar to the eighth proof for the irrationality of $\sqrt{2}$:

Proof 2. For $n \in \mathbb{N}$, set $u_n = \int_0^1 x^n e^x \mathrm{d}x$.
Using an induction and integration by part, we can prove that for $n \in \mathbb{N}$, there exist $a_n, b_n \in \mathbb{Z}$ such that $u_n = a_n + eb_n$.
Assume by contradiction that $e = \frac{p}{q}$ where $p, q \in \mathbb{N} \setminus \{0\}$. Then $0 < u_n = a_n + b_n \frac{p}{q} = \frac{qa_n + pb_n}{q}$.
Since $u_n > 0$ we get that $qa_n + pb_n \geq 1$ and that $u_n \geq \frac{1}{q}$.
Therefore $\forall n \in \mathbb{N}$, $0 < \frac{1}{q} \leq u_n \leq \int_0^1 x^n e \mathrm{d}x = \frac{e}{n+1}$.
Which is impossible. ■

A Construction of $\mathbb{R}$ via the Dedekind cuts

In this appendix, I briefly explain how to construct $\mathbb{R}$ using Dedekind cuts (but without details, just ideas).

Definition 67. We say that (A, B) is a Dedekind cut of $\mathbb{Q}$ if
- $A, B \subset \mathbb{Q}$, $A \neq \varnothing$, $B \neq \varnothing$
- $A \cap B = \varnothing$
- $A \cup B = \mathbb{Q}$
- $\forall a \in A$, $\forall b \in B$, $a < b$

Note that:
- A determines B entirely (and vice-versa), and that,
- $r \in \mathbb{Q}$ may be defined by two cuts (either $r \in A$ or $r \in B$).

To remove these ambiguities, we define a cut as follows.

Definition 68. We say that $A \subset \mathbb{Q}$ is a cut of $\mathbb{Q}$ if
- $A \neq \varnothing$
- $A \neq \mathbb{Q}$
- $\forall a \in A$, $\forall a' \in \mathbb{Q}$, $a' < a \implies a' \in A$
- A doesn't have a greatest element

Definition 69. $\mathbb{R} = \{\text{cuts of } \mathbb{Q}\}$

Example 70.
- $\sqrt{2} = \{a \in \mathbb{Q} \ : \ a < 0 \text{ or } a^2 < 2\}$
- $\mathbb{Q} \subset \mathbb{R}$, indeed we identify $q \in \mathbb{Q}$ with the cut $\{a \in \mathbb{Q} \ : \ a < q\}$.

Definition 71. For $x, y \in \mathbb{R}$, we set $x \leq y \Leftrightarrow x \subset y$.

Definition 72. For $x, y \in \mathbb{R}$, we set $x + y \coloneqq \{a + b \ : \ a \in x \text{ and } b \in y\}$.

Definition 73. For $x, y \geq 0$, we set $xy \coloneqq \{c \in \mathbb{Q} \ : \ \exists a \in x \cap \mathbb{Q}_{\geq 0}, \exists b \in y \cap \mathbb{Q}_{\geq 0}, c \leq ab\}$.
We extend the multiplication by the sign rule.

We need to prove that we constructed a (totally) ordered field, which is a little bit challenging.
Nonetheless, by construction, we can easily prove that the cut property holds:

Theorem 74. $\forall A, B \subset \mathbb{R}$,
$$\left.\begin{array}{r} A, B \neq \varnothing \\ \mathbb{R} = A \cup B \\ \forall a \in A, \forall b \in B, a < b \end{array}\right\} \implies \exists! c \in \mathbb{R}, \forall a \in \mathbb{R}, \forall b \in B, a \leq c \leq b$$

We can derive from the cut property that the least upper bound principle holds.
Let $S \subset \mathbb{R}$ be such that $S \neq \varnothing$ and S is bounded from above.
Then $B = \left\{b \in \mathbb{R} \ : \ b \text{ is an upper bound of } S\right\}$ is non-empty. So is $A = \mathbb{R} \setminus B$.
We can check that (A, B) is a Dedekind-cut of $\mathbb{R}$.
Therefore there exists $c \in \mathbb{R}$ such that $\forall a \in A$, $\forall b \in B$, $a \leq c \leq b$.
- c is an upper bound of S: otherwise there exists $s \in S$ such that $c < s$, then $a = \frac{c+s}{2} \in A$ since $a < s$. But then $a \in B$ since (A, B) is a Dedekind cut and $c < a$.
- It is the least one: let $\varepsilon > 0$ then $c - \varepsilon < c$ so $c - \varepsilon \in A$.