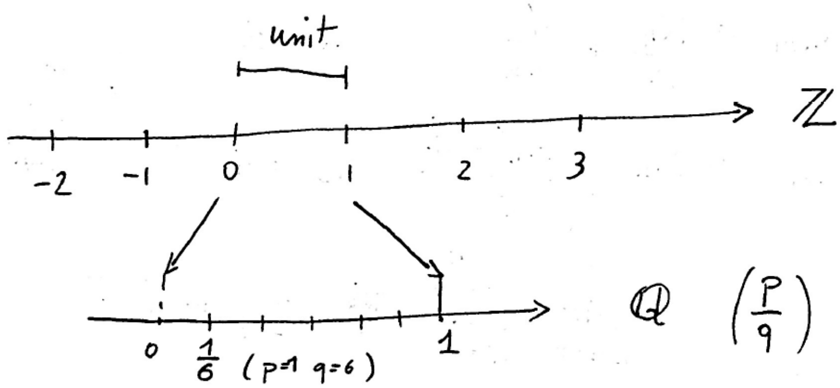
Lecture 1: Real Numbers

In this lecture we briefly discuss the set of real numbers $\mathbb{R}$, and how such set can be constructed based on successive extensions of the set of natural numbers

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

The main steps are:

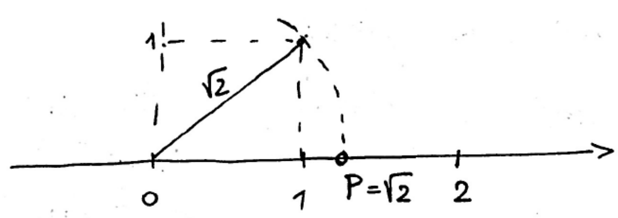
1. Construct $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$ (integer numbers).
2. Construct $\mathbb{Q} = \left\{ \frac{p}{q} \; : \; p, q \in \mathbb{Z}, \quad q \neq 0 \right\}$ (rational numbers).



Clearly[1], $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$. Rational numbers either have a finite number of decimal digits or an infinite number of decimal digits repeating periodically. For example:

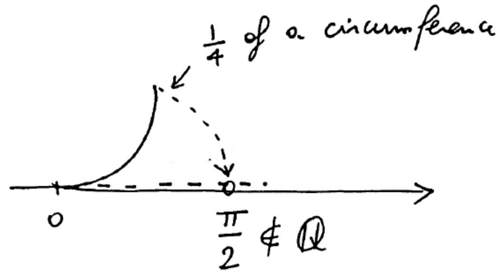
$$\frac{3}{4} = 0.75 \qquad \text{(finite number of decimals)}$$
$$\frac{1}{3} = 0.333333\ldots = 0.\overline{3} \qquad \text{(infinite number of decimals repeating periodically)}$$
$$\frac{1}{7} = 0.\underbrace{142857}\underbrace{142857}\ldots = 0.\overline{142857} \qquad \text{(infinite number of decimals repeating periodically)}$$

The set of rational numbers is not complete. In other words, there are numbers on the continuum line (horizontal line in the following figure) that are not rationals. This can be seen graphically as follows



[1]The symbol $\subset$ denotes "subset of". Note that $\mathbb{N}$ is a subset of $\mathbb{Z}$ because $\mathbb{Z}$ includes all integer numbers $\{1, 2, 3, \ldots\}$. In addition, $\mathbb{Z}$ has the negative of all integer numbers and the element zero $\{0\}$.

Similarly, the number $\pi/2$ obtained by unrolling one quarter of a unit circle over the horizonal line is not a rational number.



Remarkably, no matter how hard we try to to cover the continuum line with rational numbers we find out that the number of "holes" left to be filled is *infinite* and *uncountable* (cardinality larger than $\mathbb{N}$). Hereafter we show that there is indeed no rational number the square of which equals 2.

Theorem. There is no rational number the square of which equals 2. Equivalently, there is no rational number that equals $\sqrt{2}$.

A theorem is a statement that can be proved (or disproved) by a sequence of logical or mathematical operations. Hereafter, we provide a simple example of a proof.

Proof. Suppose that there exists a rational number p/q (irreducible fraction[2]) the square of which equals two:

$$\left(\frac{p}{q}\right)^2 = 2 \quad \Rightarrow \quad p^2 = 2q^2. \tag{1}$$

Clearly, $p^2 = 2q^2$ is an even natural number (2 times the natural number q^2 is necessarily even). This implies that p is an even integer number, and therefore can be written as

$$p = 2s \qquad \text{for some } s \in \mathbb{Z}. \tag{2}$$

Substituting equation (2) into (1) yields

$$\frac{2^2 s^2}{q^2} = 2 \quad \Rightarrow \quad q^2 = 2s^2 \quad \Rightarrow \quad q\,\text{even}. \tag{3}$$

But this contradicts the fact that p/q is an irreducible fraction. In fact we just concluded that both p and q are divisible by 2 since they are both even numbers. In summary, the assumption that there exists a rational number p/q equals to $\sqrt{2}$ yields a contradiction, and therefore the assumption must be wrong, meaning that such a rational number cannot exist.

□

There are many other examples of numbers that cannot be represented as a ratio between two integer number (i.e., rationals). Such numbers are called *irrational numbers*, and they have an infinite number of decimals (non-repeating). Moreover, as mentioned above, there is an infinite number irrational numbers. Well known examples of irrational numbers are: $\pi = 3.141592653\cdots$, $\sqrt{2} = 1.41421356\cdots$, $\sqrt{3} = 1.73205080\cdots$, $e = 2.71828182845\cdots$ (Napier number).

[2]An irreducible fraction is a fraction that cannot be simplified any further. For example, 3/2 is an irreducible fraction while 6/4 is not an irreducible fraction as both the numerator and the denominator can be divided by 2 to obtain 3/2.

Remarkably, all irrational numbers can be obtained as limits points of suitable sequences of rational numbers. For example,

$$\pi = 4\sum_{n=0}^{\infty}\frac{(-1)^n}{2n+1} = 4\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\cdots\right) \qquad \text{(Leibnitz sequence)}$$

$$e = \sum_{n=0}^{\infty}\frac{1}{n!} = 1+1+\frac{1}{2}+\frac{1}{6}+\frac{1}{24}+\cdots$$

Similarly, $\sqrt{2}$ can be obtained by iterating (an infinite number of times) the following sequence of rational numbers:

$$S_{n+1} = \frac{S_n}{2}+\frac{1}{S_n} \qquad S_0 = 1 \tag{4}$$

i.e.,

$$S_0 = 1, \qquad S_1 = \frac{3}{2} = 1.5, \qquad S_2 = \frac{17}{12} = 1.41\overline{6}, \qquad S_3 = \frac{577}{408} = 1.414\overline{2156862745098039}, \quad \ldots$$

The sequences above are not unique, meaning that there are many other sequences of rationals converging to the same irrationals. In any case, such sequences exist, and they can represent (in their limit) all irrational numbers[3]. By adding the set of irrational numbers (denoted by $\mathbb{I}$), which is uncountable, to the set of the rationals $\mathbb{Q}$ we obtain the set of *real numbers*:

$$\mathbb{R} = \mathbb{Q}\cup\mathbb{I} \tag{5}$$

A remarkable result of number theory says that both $\mathbb{Q}$ and $\mathbb{I}$ are dense in $\mathbb{R}$. This means that any real number can be obtained as limit point of sequences of rational numbers or sequences of irrational numbers. Moreover, between any two distinct real numbers there always exists a rational number and an irrational one.

Axiomatic definition of $\mathbb{R}$

The set of real numbers can be defined in an axiomatic way. An axiom is statement or proposition which is regarded as being established, accepted, or self-evidently true. Hence, by defining $\mathbb{R}$ in terms of axioms we specify properties of $\mathbb{R}$ that are self-evidently true. Such properties will be used in the sequel to properly define the set of complex numbers $\mathbb{C}$ (next lecture).

Field Axioms. The set of real number $\mathbb{R}$ is a field, i.e., it is a set in which we define two operations (addition "+" and multiplication[4]) with the following properties:

1. Associative property: $\forall x, y, z \in \mathbb{R}, \quad (x+y)+z = x+(y+z) \quad$ and $\quad (xy)z = x(yz)$.
2. Commutative property: $\forall x, y \in \mathbb{R},\ x+y = y+x \quad$ and $\quad xy = yx$.
3. Additive neutral element: There exists an element of $\mathbb{R}$, denoted by 0, such that $\forall x \in \mathbb{R}$, $x+0 = x$.

[3]The sequences are actually used in practice to compute approximations of irrational numbers. For example, in 2016 Ron Watkins used the sequence (4) to compute 10 trillion digits of $\sqrt{2}$ (see `http://www.numberworld.org/digits/Sqrt(2)/`).

[4]The multiplication operation between two elements $x, y \in \mathbb{R}$ is denoted simply as xy.

4. Multiplicative neutral element: There exists an element of $\mathbb{R}$, denoted by 1, such that $\forall x \in \mathbb{R}$, $1x = x$.

5. Inverse with respect to addition: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}|\ x + y = 0$ $(y = -x)$ (y is the opposite of x).

6. Inverse with respect to multiplication: $\forall x \in \mathbb{R} \setminus \{0\}, \exists y \in \mathbb{R}|\ x \cdot y = 1$ (y is the inverse of x).

7. Distributive property of multiplication: $\forall x, y, z \in \mathbb{R},\ x(y + z) = xy + xz$.

Remark: The set $\mathbb{R}$ is closed under addition and multiplication, meaning that the result of such operations is still a real number. In general, any set satisfying properties (1)-(7) is a called *field*. In particular, it is easy to see that: 1) $\mathbb{N}$ is not a field; 2) $\mathbb{Z}$ is not a field (the inverse with respect to multiplication is not in $\mathbb{Z}$); 3) $\mathbb{Q}$ is a field; 4) $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ is not a field (the product of two irrationals can be an integer $\sqrt{2}\sqrt{2} = 2$).

By using the field axioms it is easy define subtraction and division between two real numbers as:

Subtraction: $\forall x, y \in \mathbb{R},\ x - y = x + (-y)$ (subtraction seen as adding the opposite of y).

Division: $\forall x, y \in \mathbb{R},\ y \neq 0,\ x/y = xy^{-1}$ (division seen as multiplying by the inverse of y).

Ordering Axioms. The field of real numbers $\mathbb{R}$ is totally ordered, i.e., we can define in $\mathbb{R}$ an ordering relation $\leq$ such that:

1. $x \leq y \quad \Rightarrow \quad x + z \leq y + z, \qquad \forall z \in \mathbb{R}$.

2. $x \leq y \quad \Rightarrow \quad xz \leq yz, \qquad \forall z \geq 0$.

Remark: The ordering axioms say that all elements of $\mathbb{R}$ are ordered, i.e., we can always tell which element is bigger or smaller than any other element.

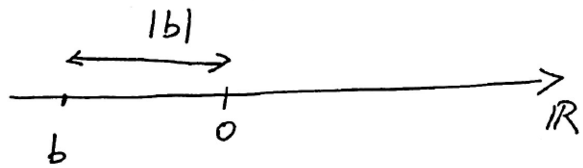
Completeness Axiom. $\mathbb{R}$ is a field that is totally ordered and complete. "Complete" means that for every subsets $A, B \subseteq \mathbb{R}$ not empty and separated (i.e., such that $a \leq b\ \forall a \in A$ and $\forall b \in B$) there exists at least one $c \in \mathbb{R}$ such that $a \leq c \leq b$.

Remark: The completeness axiom assures that the set $\mathbb{R}$ has no "holes" in it. Also, it can be shown that between two real numbers there is always an irrational and a rational, and between two rational numbers there is always a real number and an irrational number.

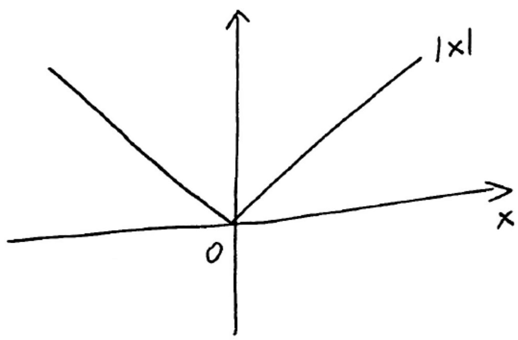
Based on the Field, Ordering and Completeness axioms it is possible to derive other important properties of $\mathbb{R}$. For example for all $x, y \geq 0$ we have that $x^2 = y^2 \Leftrightarrow x = y$ and $x^2 \leq y^2 \Leftrightarrow x \leq y$. At this point we define on $\mathbb{R}$ an important function, i.e., the **absolute value**

$$|\cdot| : \mathbb{R} \to \mathbb{R}^+. \tag{6}$$

Here $\mathbb{R}^+$ denotes the set of non-negative real numbers, i.e., $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\}$. The absolute value function takes in any real number b and it returns the length of the segment that connects the origin to b.



$$|\cdot| : \mathbb{R} \to \mathbb{R}^+$$



The absolute value function satisfies a certain number of properties summarized in the following theorem. Each of the properties can be proved based on the definition of $|\cdot|$.

Theorem (Properties of the absolute value)**.** Let $a, b \in \mathbb{R}$. Then we have

1. $|a| \geq 0$
2. $|a| = 0 \Leftrightarrow a = 0$
3. $|a| = |-a|$
4. $-|a| \leq a \leq |a|$
5. $|a|^2 = a^2$
6. $|ab| = |a||b|$
7. $|a + b| \leq |a| + |b|$ (Triangle inequality)
8. $|a + b| \geq ||a| - |b||$

By using the definition of absolute value we can define closed and open intervals of the real line with endpoint a and b ($a, b \in \mathbb{R}$, $a < b$) as

$$[a, b] = \{x \in \mathbb{R} |\ a \leq x \leq b\} = \{x \in \mathbb{R} : \left| x - \frac{a+b}{2} \right| \leq \frac{b-a}{2}\} \quad \text{(closed interval)} \tag{7}$$

$$]a, b[= \{x \in \mathbb{R} |\ a < x < b\} = \{x \in \mathbb{R} : \left| x - \frac{a+b}{2} \right| < \frac{b-a}{2}\} \quad \text{(open interval)} \tag{8}$$

Solution to linear an nonlinear equations. In general, it is good practice to specify in which space we are looking for solutions of a certain equation. For instance, the following linear equation

$$2x = 1 \tag{9}$$

has no solution in $\mathbb{N}$ and no solution in $\mathbb{Z}$, but it has a unique solution in $\mathbb{Q}$ equal to $x = 1/2$, and of course a unique solution in $\mathbb{R}$ (since $\mathbb{Q} \subset \mathbb{R}$). Many nonlinear equations, however, do not admit a solution in $\mathbb{R}$. For example, the following polynomial (quadratic) equation

$$x^2 + 1 = 0 \tag{10}$$

has no solution in $\mathbb{R}$. In fact, we have seen that the square of any real number x is non-negative, i.e., $x^2 \geq 0$ for all $x \in \mathbb{R}$. Hence, there is no element in $\mathbb{R}$ such that $x^2 = -1$, and therefore (10) has no solution in $\mathbb{R}$. If we are still interested in defining solutions to (10), then we need to utilize a different set of numbers. In particular, such a set should include particular type of numbers the square of which is negative and real. As we ill see those numbers are called *imaginary numbers*, and will be described in detail in the next lecture. Imaginary numbers are a subset of a more general set of numbers which is *complex numbers* and denoted as $\mathbb{C}$. Historically, complex numbers were developed to make sense of solutions of polynomial equations (i.e., roots of polynomials).

Theorem (Fundamental theorem of algebra)**.** Every non-constant single-variable polynomial with real or complex coefficients has at least one complex root.

By applying this theorem recursively, it can be shown that every polynomial of degree n has exactly n complex roots (which may not be all distinct).

Complex numbers and complex functions can be found in a variety of applications, e.g., series expansions of periodic functions, signal processing, harmonic analysis, quantum mechanics (e.g., Schrödinger equation), fluid dynamics, conformal maps (e.g., Joukowsky maps - used to understand some principles of airfoil design), nonlinear dynamics and control, image processing, wave propagation, etc.