# Math 140A - Notes

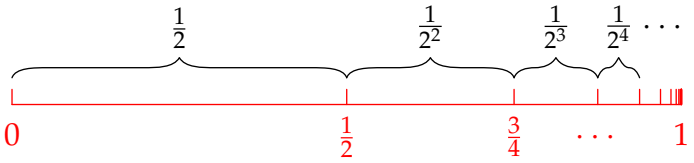
Neil Donaldson

January 16, 2025

## Introduction

Analysis is one of the major sub-disciplines of mathematics, concerned with continuity, limits, calculus, and accurate approximations.

Analytic ideas date back thousands of years. For instance, Archimedes (c. 287–212 BC) used limit-type approaches to approximate the circumference of a circle and to compute the area under a parabola.[1] Philosophical objections to such ideas are just as old: how can it make sense to sum infinitely many infinitesimally small quantities? This was part of a deeper debate among the ancient Greeks and other cultures: is the matter comprising the natural world *atomic* (consisting of minute, discrete, indivisible objects) or *continuous* (arbitrarily and infinitely divisible). Several of Zeno's famous paradoxes ($5^{\text{th}}$ C. BC) grapple with such difficulties: *Achilles and the Tortoise* is essentially an argument that the infinite series $\sum_{n=1}^{\infty} \frac{1}{2^n} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots$ is meaningless.




As the picture suggests, with modern definitions it makes sense for this sum to evaluate to 1.

The development of calculus by Newton, Leibniz and others in the late 1600s permitted the easy application of infinitesimal ideas to important problems in the sciences, though they did not properly address the ancient philosophical concerns. The main subject of this course (and its sequel) is the rigorous logical development of the foundations of calculus: the triumph of $18^{\text{th}}$–$19^{\text{th}}$ century mathematics. The critical notions of limit and continuity only became settled in during the early 1800s (courtesy of Bolzano, Cauchy, Weierstrass and others), with another 50 years passing before Riemann's thorough description of the definite integral.

In this course we consider sequences, limits, continuity and infinite series, with power series, differentiation and integration relegated to the sequel. We begin with something more basic: to numerically measure continuous quantities, we need to familiarize ourselves with the *real numbers*. A concrete description is difficult, so we build up to it via the natural numbers and the rationals…

[1] Archimedes' circle is reminiscent of Riemann sums; his parabola requires evaluation of the infinite series $\sum_{n=0}^{\infty} \frac{1}{4^n} = \frac{4}{3}$.

# 1 Completeness

## 1.1 The Set $\mathbb{N}$ of Natural Numbers

You've been using the natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$ since you first learned to count. In mathematics, these must be *axiomatically* described. Here is one approach.

**Axioms 1.1 (Peano).** The natural numbers are a set $\mathbb{N}$ satisfying the following properties:

1. (Non-emptiness) $\mathbb{N}$ is non-empty.
2. (Successor function) There exists a function $f : \mathbb{N} \to \mathbb{N}$. This is usually denoted '$+1$' so that we may write,
$$n \in \mathbb{N} \implies n + 1 \in \mathbb{N}$$
3. (Initial element) The successor function $f$ is *not surjective.* Otherwise said, there is an element $1 \notin \text{range } f$ which is not the successor of any element.[2]
4. (Unique predecessor/order) $f$ is *injective.* Otherwise said,
$$m + 1 = n + 1 \implies m = n$$
5. (Induction) Suppose $A \subseteq \mathbb{N}$ is a subset satisfying
   (a) $1 \in A$, (b) $n \in A \implies n + 1 \in A$.
   Then $A = \mathbb{N}$.

Axioms 1–4 state that $\mathbb{N}$ is defined by repeatedly adding 1 to the initial element; for instance
$$3 := f\big(f(1)\big) = f(1 + 1) = (1 + 1) + 1$$
Parts (a) and (b) of axiom 5 are the familiar *base case* and *induction step* a standard induction: let $P_n$ be the proposition '$n \in A$' to recover the usual form of the *Principle of Mathematical Induction.*

**Example 1.2.** Prove that $7^n - 4^n$ is divisible by 3 for all $n \in \mathbb{N}$.
Let $A$ be the set of natural numbers for which $7^n - 4^n$ is divisible by 3. It is required to prove that $A = \mathbb{N}$.

(a) If $n = 1$, then $7^1 - 4^1 = 3$, whence $1 \in A$.

(b) Suppose $n \in A$. Then $7^n - 4^n = 3\lambda$ for some $\lambda \in \mathbb{N}$. But then
$$\begin{aligned} 7^{n+1} - 4^{n+1} &= 7 \cdot 7^n - 4^{n+1} = 7(3\lambda + 4^n) - 4^{n+1} = 3 \cdot 7\lambda + (7 - 4) \cdot 4^n \\ &= 3\big(7\lambda + 4^n\big) \end{aligned}$$
is divisible by 3. It follows that $n + 1 \in A$.

Appealing to axiom 5, we see that $A = \mathbb{N}$, hence result.

[2] By convention, the first natural number is 1; we could use 0, $x$, $\alpha$, or any symbol you wish!

**What about the integers?** The integers satisfy only axioms 1, 2 and 4. For instance:

$\not{3}$. The function $f : \mathbb{Z} \to \mathbb{Z} : n \mapsto n+1$ is surjective (indeed bijective/invertible). The 'initial element' $1 \in \mathbb{N}$ is the successor of $0 \in \mathbb{Z}$.

Reversing this observation provides an explicit construction of $\mathbb{Z}$ from $\mathbb{N}$: simply extend the successor function $f$ so that every element has a unique predecessor: 0 is the unique predecessor of 1, $-1$ the unique predecessor of 0, etc. In essence we are forcing $f(n) = n+1$ to be bijective!

**Exercises 1.1.** *Key concepts/results: Peano's Axioms, Induction*
Most of these exercises are to refresh your memory of induction. Use either the language of Peano's axiom 5, or the (possibly) more familiar base-case/induction-step formulation.

1. Prove that $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$ for all natural numbers $n$.
2. Prove that $3 + 11 + \cdots + (8n-5) = 4n^2 - n$ for all $n \in \mathbb{N}$.
3. (a) Guess a formula for $1 + 3 + \cdots + (2n-1)$ by evaluating the sum for $n = 1, 2, 3$, and 4. (*For $n = 1$ the sum is simply 1*)
   (b) Prove your formula using mathematical induction.
4. Prove that $11^n - 4^n$ is divisible by 7 for all $n \in \mathbb{N}$.
5. The principle of mathematical induction can be extended as follows. A list $P_m, P_{m+1}, \ldots$ of propositions is true provided (i) $P_m$ is true, (ii) $P_{n+1}$ is true whenever $P_n$ is true and $n \geq m$.
   (a) Prove that $n^2 > n+1$ for all integers $n \geq 2$.
   (b) Prove that $n! > n^2$ for all integers $n \geq 4$. (*recall that $n! = n(n-1)\cdots 2 \cdot 1$*)
6. Prove $(2n+1) + (2n+3) + (2n+5) + \cdots + (4n-1) = 3n^2$ for all $n \in \mathbb{N}$.
7. For each $n \in \mathbb{N}$, let $P_n$ denote the assertion "$n^2 + 5n + 1$ is an even integer".
   (a) Prove that $P_{n+1}$ is true whenever $P_n$ is true.
   (b) For which $n$ is $P_n$ actually true? What is the moral of this exercise?
8. For $n \in \mathbb{N}$, let $n!$ denote the factorial function ($0! = 1$) and define the binomial coefficient
   $$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad \text{for} \quad k = 0, 1, \ldots, n$$
   The *binomial theorem* asserts that, for all $n \in \mathbb{N}$,
   $$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k = a^n + na^{n-1}b + \frac{n(n-1)}{2}a^{n-2}b^2 + \cdots + nab^{n-1} + b^n$$
   (a) Show that $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ for $k = 1, 2, \ldots, n$.
   (b) Prove the binomial theorem by induction.
9. Show that Peano's induction axiom is *false* for the set of integers $\mathbb{Z}$ by exhibiting a *proper subset* $A \subset \mathbb{Z}$ which satisfies conditions (a) and (b).
10. Consider $\mathbb{Z}_3 = \{0, 1, 2\}$ under addition modulo 3. That is,
    $$0+1 = 1, \quad 1+1 = 2, \quad 2+1 = 0$$
    Which of Peano's axioms are satisfied?

## 1.2 The Set $\mathbb{Q}$ of Rational Numbers

The rational numbers may be defined in several ways. For instance, we could consider the set of relatively prime ordered pairs

$$\mathbb{Q} = \{(p,q) : p \in \mathbb{Z},\ q \in \mathbb{N},\ \gcd(p,q) = 1\} \subseteq \mathbb{Z} \times \mathbb{N}$$

Things seem more familiar if we write $\frac{p}{q}$ instead of $(p,q)$ and adopt the convention that $\frac{\lambda p}{\lambda q} = \frac{p}{q}$ for any non-zero $\lambda \in \mathbb{Z}$. The usual operations $(+, \cdot,$ etc.$)$ are easily defined, consistently with those for the integers (Exercise 6).

An alternative approach involves equations. Each *linear equation* $qx - p = 0$ where $p, q \in \mathbb{Z}$ and $q \neq 0$ corresponds to a rational number. For example

$$13x + 27 = 0 \leftrightsquigarrow x = -\frac{27}{13}$$

Of course the equation $26x + 54 = 0$ *also* corresponds to the same rational number!

Extending this process naturally leads us to consider higher degree polynomials.

**Definition 1.3.** A number $x$ is *algebraic* if it satisfies an equation of the form[3]

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \qquad (*)$$

for some integers $a_0, \ldots, a_n$.

**Examples 1.4.** 1. $\sqrt{2}$ is algebraic since it satisfies the equation $x^2 - 2 = 0$.

2. $x = \sqrt[5]{7 + \sqrt{3}}$ is also algebraic:

$$x^5 - 7 = \sqrt{3} \implies (x^5 - 7)^2 = 3 \implies x^{10} - 14x^5 + 46 = 0$$

The next result is helpful for deciding whether a given number is rational and can assist with factorizing polynomials.

**Theorem 1.5 (Rational Roots).** *Suppose $a_0, \ldots, a_n \in \mathbb{Z}$ and that $x \in \mathbb{Q}$ satisfies $(*)$. If $x = \frac{p}{q}$ is rational, written in lowest terms, then $p \mid a_0$ and $q \mid a_n$.*

*Proof.* Substitute $x = \frac{p}{q}$ into the polynomial equation and multiply through by $q^n$ to see that

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

This is an equation *in integers.* All terms except the last contain a factor of $p$, whence $p \mid a_0 q^n$. Since $\gcd(p,q) = 1$, it follows that $p \mid a_0$. The result for $q$ is almost identical: all but the first term above has a factor of $q$. ∎

[3] You should be alarmed by this! We seem to have given up *constructing* new numbers and instead are merely *describing* their properties. No matter, a construction of the real numbers will come later.

**Examples 1.6.** 1. We prove that $\sqrt{2}$ is irrational. Plainly $x = \sqrt{2}$ satisfies the polynomial equation $x^2 - 2 = 0$. If $\sqrt{2} = \frac{p}{q}$ were rational in lowest terms, then the rational roots theorem forces

$$p \mid 2 \quad \text{and} \quad q \mid 1 \implies \sqrt{2} \in \{\pm 1, \pm 2\}$$

Since none of the values $\pm 1, \pm 2$ satisfy $x^2 - 2 = 0$, we have a contradiction.

2. $y = (\sqrt{3} - 1)^{1/3}$ satisfies $(y^3 + 1)^2 = 3$, whence $y^6 + 2y^3 - 2 = 0$. If $y = \frac{p}{q}$ were rational in lowest terms, then $p \mid 2$ and $q \mid 1$, whence $y = \pm 1, \pm 2$; none of which satisfy the polynomial.

3. $z = \left(\frac{4+\sqrt{3}}{5}\right)^{1/2}$ satisfies $5z^2 - 4 = \sqrt{3}$, from which $25z^4 - 40z^2 + 13 = 0$. If $z = \frac{p}{q}$ were rational in lowest terms, then $p \mid 13$ and $q \mid 25$. There are twelve possibilities: it is tedious to check, but none satisfy the required polynomial,

$$z = \pm 1,\ \pm 13,\ \pm\tfrac{1}{5},\ \pm\tfrac{13}{5},\ \pm\tfrac{1}{25},\ \pm\tfrac{13}{25}$$

In this case it is easier to bypass the theorem: if $z \in \mathbb{Q}$ then $\sqrt{3} = 5z^2 - 4$ would also be rational!

4. We use the theorem to factorize the polynomial $3x^3 + x^2 + x - 2 = 0$. If $x = \frac{p}{q}$ is a rational root, then $p \mid 2$ and $q \mid 3$ give several possibilities:

$$x \in \left\{\pm 1, \pm 2, \pm\tfrac{1}{3}, \pm\tfrac{2}{3}\right\}$$

It doesn't take long to check that $x = \frac{2}{3}$ is the only rational root. A factor of $3x - 2$ may be extracted by long division to obtain

$$3x^3 + x^2 + x - 2 = (3x - 2)(x^2 + x + 1)$$

The quadratic has no real roots: absent complex numbers, the factorization is complete.

It is far from clear that non-algebraic (*transcendental*) numbers exist: $e$ and $\pi$ are the most famous. These satisfy no polynomial equation with integer coefficients, though demonstrating such is tricky.

**Exercises 1.2.** *Key concepts: Algebraic Numbers, Rational Roots Theorem/Testing for Irrationality*

1. Describe all linear equations corresponding to the rational number $\frac{101}{29}$.
2. Show that $\sqrt{3}$, $\sqrt{5}$ and $\sqrt{24}$ are not rational numbers: what are the relevant polynomials?
3. Show that $2^{1/3}$ and $13^{1/4}$ are not rational numbers.
4. Show that $(2 + \sqrt{2})^{1/2}$ and $(5 - \sqrt{3})^{1/3}$ are irrational.
5. Explain why $4 - 7b^2$ must be rational if $b$ is rational.
6. Given rational numbers $(p, q)$, $(r, s)$ as ordered pairs, what are $(p, q) + (r, s)$ and $(p, q) \cdot (r, s)$?
7. Let $n \in \mathbb{N}$. Use the rational roots theorem to prove that $\sqrt{n} \in \mathbb{Q} \iff \sqrt{n} \in \mathbb{N}$.
8. In the proof of the rational roots theorem, explain why the condition $\gcd(p, q) = 1$ allows us to conclude that $p \mid a_0 q^n \implies p \mid a_0$

## 1.3 Ordered Fields

We have thus far formally constructed the natural numbers and used them to build the integers and rational numbers. It is a significantly greater challenge to *construct* the real numbers. We start by thinking about ordered fields, of which both $\mathbb{Q}$ and $\mathbb{R}$ are examples.

**Axioms 1.7.** A *field* $\mathbb{F}$ is a set with two binary operations $+, \cdot$ which satisfy (for all $a, b, c \in \mathbb{F}$),[4]

| | Addition | Multiplication |
|---|---|---|
| Closure | $a + b \in \mathbb{F}$ | $ab \in \mathbb{F}$ |
| Associativity | $a + (b + c) = (a + b) + c$ | $a(bc) = (ab)c$ |
| Commutativity | $a + b = b + a$ | $ab = ba$ |
| Identity | $\exists 0 \in \mathbb{F}$ such that $a + 0 = a$ | $\exists 1 \in \mathbb{F}$ such that $a \cdot 1 = a$ |
| Inverse | $\exists -a \in \mathbb{F}$ such that $a + (-a) = 0$ | If $a \neq 0$, $\exists a^{-1} \in \mathbb{F}$ such that $aa^{-1} = 1$ |
| Distributivity | $a(b + c) = ab + ac$ | |

A field $\mathbb{F}$ is *ordered* if we also have a binary relation $\leq$ which satisfies (again for all $a, b, c \in \mathbb{F}$):

O1 $a \leq b$ or $b \leq a$

O2 $a \leq b$ and $b \leq a \implies a = b$

O3 $a \leq b$ and $b \leq c \implies a \leq c$

O4 $a \leq b \implies a + c \leq b + c$

O5 $a \leq b$ and $0 \leq c \implies ac \leq bc$

For an ordered field, the symbol $<$ is used in the usual manner: $x < y \iff x \leq y$ and $x \neq y$.

As with Peano's axioms for the natural numbers, these are not worth memorizing. Instead you should quickly check that you believe all of them for your current understanding of the real numbers; you can't *prove* anything since the real numbers are yet to be defined!

**Example 1.8.** It is worth considering the rational numbers in a little more detail. These inherit a natural ordering from $\mathbb{Z}$ and $\mathbb{N}$:

$$\frac{p}{q} \leq \frac{r}{s} \iff ps \leq qr \qquad \text{(remember that } q, s > 0\text{)}$$

It is now possible, though tedious, to *prove* that each of the axioms of an ordered field holds for $\mathbb{Q}$, using only basic facts about multiplication, addition and ordering *within the integers.* For instance,

[4] Write multiplication $\cdot$ as juxtaposition unless necessary, and use the common shorthand $a^2 = a \cdot a$. The field axioms are very easy to remember if you know some abstract algebra:

- The addition axioms say that $(\mathbb{F}, +)$ is an abelian group.
- The multiplication axioms say that $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group.
- The distributive axiom describes how addition and multiplication interact.

*Commutativity of Multiplication* Given $a = \frac{p}{q}$ and $b = \frac{s}{t}$ rational, we have

$$ab = \frac{ps}{qt} = \frac{sp}{tq} = ba$$

since multiplication of integers (numerator and denominator) is commutative.

O3 Suppose $a \leq b$ and $b \leq c$. Write $a = \frac{p}{q}$, $b = \frac{r}{s}$ and $c = \frac{t}{u}$ where all three denominators are positive. By assumption,

$$\begin{aligned} ps \leq qr \text{ and } ru \leq st &\implies psu \leq qru \leq qst \\ &\implies pu \leq qt && \text{(divide by } s \neq 0) \\ &\implies a = \frac{p}{q} \leq \frac{t}{u} = c \end{aligned}$$

**Basic Results about ordered fields**

As with the axioms of an ordered field, these are not worth memorizing.

**Theorem 1.9.** *Let $\mathbb{F}$ be a ordered field with at least two elements $0 \neq 1$. Then:*

1. $a + c = b + c \implies a = b$
2. $a \cdot 0 = 0$
3. $(-a)b = -(ab)$
4. $(-a)(-b) = ab$
5. $ac = bc$ *and* $c \neq 0 \implies a = b$
6. $ab = 0 \implies a = 0$ *or* $b = 0$
7. $a \leq b \implies -b \leq -a$
8. $a \leq b$ *and* $c \leq 0 \implies bc \leq ac$
9. $0 \leq a$ *and* $0 \leq b \implies 0 \leq ab$
10. $0 \leq a^2$
11. $0 < 1$
12. $0 < a \implies 0 < a^{-1}$
13. $0 < a < b \implies 0 < b^{-1} < a^{-1}$

All these statements should be intuitive for the fields $\mathbb{Q}$ and $\mathbb{R}$. Try proving a few using only the axioms; they are most easily done in the order presented. For instance, part 2 might be proved as follows:

$$\begin{aligned} & a \cdot 0 + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 && \text{(additive identity/distibutive axioms)} \\ \implies & 0 = a \cdot 0 && \text{(part 1)} \end{aligned}$$

We finish with a final useful ingredient.

**Definition 1.10.** In an ordered field $\mathbb{F}$, the *absolute value* of an element $a$ is

$$|a| := \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

**Theorem 1.11.** *In any ordered field:*

1. $|a| \geq 0$
2. $|ab| = |a| \cdot |b|$
3. $|a+b| \leq |a| + |b|$ *($\triangle$-inequality)*
4. $|a-b| \geq ||a| - |b||$ *(reverse/extended $\triangle$-inequality)*

All parts are straightforward if you consider the $\pm$-cases separately for $a, b$.

**Exercises 1.3.** *Key concepts: Ordered Field ($\mathbb{Q}$ an example arising naturally from $\mathbb{Z}$), $\triangle$-inequality*

1. Which of the axioms of an ordered field fail for $\mathbb{N}$? For $\mathbb{Z}$?
2. Prove parts 11 and 13 of Theorem 1.9.
   (*Hint: You can use any of the parts that come before...*)
3. (a) Prove that $|a+b+c| \leq |a| + |b| + |c|$ for all $a, b, c \in \mathbb{R}$.
   (*Hint: Apply the triangle inequality twice. Don't consider eight separate cases!*)
   (b) For any $a_1, \ldots, a_n \in \mathbb{R}$, use induction to prove
   $$|a_1 + a_2 + \cdots + a_n| \leq |a_1| + |a_2| + \cdots + |a_n|$$
4. (a) Show that $|b| < a \iff -a < b < a$.
   (b) Show that $|a-b| < c \iff b - c < a < b + c$.
   (c) Show that $|a-b| \leq c \iff b - c \leq a \leq b + c$.
5. Let $a, b \in \mathbb{R}$. Show that if $a \leq b_1$ for every $b_1 > b$, then $a \leq b$.
   (*Hint: draw a picture if you're stuck. This is a very important example!*)
6. In an ordered field, suppose that $0 \leq a$ and $0 \leq b$. Explain carefully why $0 \leq a + b$.
7. Following Example 1.8, prove that $\mathbb{Q}$ satisfies axiom O5.
   (*Hint: if $a = \frac{p}{q}$, etc., what is meant by $ac \leq bc$?*)
8. (Hard!) The complex numbers $\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$ form a field. The lexicographic ordering of $\mathbb{C}$ is defined by
   $$x + iy \leq p + iq \iff \begin{cases} x < p \text{ or} \\ x = p \text{ and } y \leq q \end{cases}$$
   Which of the order axioms O1–O5 are satisfied by the lexicographic ordering?
   (*Provide a counter-example if an axiom is not satisfied; don't prove your claims if an axiom is satisfied.*)

## 1.4 The Completeness Axiom, or Least Upper Bound Principle

Though we haven't provided an explicit *definition* of the real numbers, you should be comfortable that both $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields. We now ask how these might be distinguished *axiomatically*. Perhaps surprisingly, only one additional axiom is required! We first need some terminology.

**Definition 1.12 (Maxima, Minima & Boundedness).** Let $S \subseteq \mathbb{R}$ be non-empty.

1. $S$ is *bounded above* if it has an *upper bound* $M$:

   $$\exists M \in \mathbb{R} \text{ such that } \forall s \in S,\ s \leq M$$

2. We write $M = \max S$, the *maximum* of $S$, if $M$ is an upper bound for $S$ **and** $M \in S$.
3. $S$ *bounded below*, a *lower bound* $m$, and the *minimum* $\min S$ are defined similarly.
4. $S$ is *bounded* if it is bounded both above and below. It is *bounded by* $M$ if

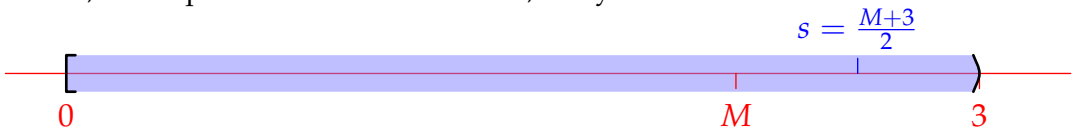
   $$\forall s \in S,\ |s| \leq M \qquad (M \text{ is an upper bound, } -M \text{ a lower bound})$$

**Examples 1.13.** 1. If $S$ is a finite set, then it is bounded and has both a maximum and a minimum. For instance, $S = \{-3, \pi, 12\}$ has $\min S = -3$ and $\max S = 12$.

2. $\mathbb{N}$ has minimum 1, but no maximum. $\mathbb{Z}$ and $\mathbb{Q}$ have neither: both are *unbounded*.

3. The half-open interval $S = [0, 3)$ is bounded, e.g. by $M = 5$; it has minimum 0 but no maximum. While this last is intuitive, it is worth giving an explicit argument, in this case by contradiction.[5]

   Suppose $M = \max S$ exists; necessarily $0 \leq M < 3$. We draw a picture to get the lay of the land: since $M \in S$, we've placed it *inside* the interval, away from 3.

   The crux of the argument is to observe that there must be some $s \in S$ which is *larger* than $M$, the natural choice being the average $s := \frac{1}{2}(M + 3)$. Now observe that

   $$3 - s = s - M = \frac{1}{2}(3 - M) > 0$$

   In particular, $s \in S$ and $s > M$. Since $S$ contains an element larger than $M$, it follows that $M$ cannot be the maximum of $S$. In conclusion, $S$ has no maximum.

**Lemma 1.14.** 1. *If $M$ is an upper bound for $S$, so is $M + \varepsilon$ for any $\varepsilon \geq 0$.*

2. *If $M = \max S$ exists, then it is unique.*

Try proving these basic facts yourself.

[5] $S$ has a maximum means: $\exists M \in S$ such that $\forall s \in S,\ s \leq M$. We prove the negation $\forall M \in S, \exists s \in S$ such that $s > M$.

**Example 1.15.** In a variation on the previous example, we show that the set

$$S = \mathbb{Q} \cap [0, \sqrt{2}) = \{x \in \mathbb{Q} : 0 \leq x < \sqrt{2}\}$$

has no maximum. The approach is similar to before: given a hypothetical maximum $M$, we find some $s \in S$ between $M$ and $\sqrt{2}$. The challenge is that we can't use the *average* $\frac{1}{2}(M + \sqrt{2})$: this isn't rational (*why?*) and so doesn't lie in $S$!

To fix this, we informally construct a sequence. Define $s_n$ to be $\sqrt{2}$ to $n$ decimal places:

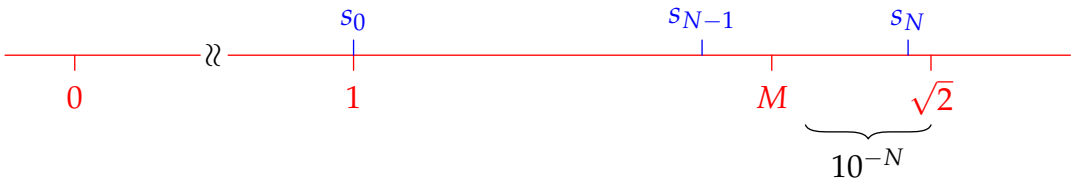
$$s_0 = 1, \quad s_1 = 1.4 = \frac{14}{10}, \quad s_2 = 1.41 = \frac{141}{100}, \quad s_3 = 1.414 = \frac{1414}{1000}, \quad \dots$$

Since any finite decimal is rational and $0 \leq s_n < \sqrt{2}$, we see that $s_n \in S$. Moreover, $\sqrt{2} - s_n \leq 10^{-n}$ can be made arbitrarily small by choosing $N$ sufficiently large.

Now suppose $M = \max S$ exists. Since $M \in S$, we have $M < \sqrt{2}$. Choose any $N \in \mathbb{N}$ large enough so that $10^{-N} < \sqrt{2} - M$ (any integer $N > -\log_{10}(\sqrt{2} - M)$ will do!). Certainly $s_N \in S$ and moreover,

$$\sqrt{2} - s_N \leq 10^{-N} < \sqrt{2} - M \implies M < s_N$$

The purported maximum $M$ is plainly not an upper bound for $S$: contradiction.

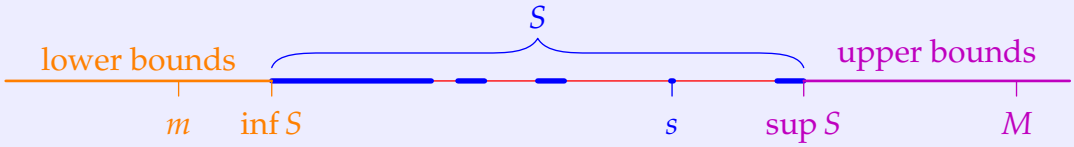



### Suprema and Infima

We generalize the idea of maximum and minimum values to any bounded sets.

**Definition 1.16.** Let $S \subseteq \mathbb{R}$ be non-empty.

1. If $S$ is bounded above, its *supremum* $\sup S$ is its *least upper bound*. Otherwise said,
   (a) $\sup S$ is an upper bound: $\forall s \in S,\ s \leq \sup S$,
   (b) $\sup S$ is the least such: if $M$ is an upper bound, then $\sup S \leq M$.
2. Similarly, if $S$ is bounded below, its *infimum* $\inf S$ is its *greatest lower bound*:
   (a) $\inf S$ is a lower bound: $\forall s \in S,\ \inf S \leq s$,
   (b) $\inf S$ is the greatest such: if $m$ is a lower bound, then $m \leq \inf S$.

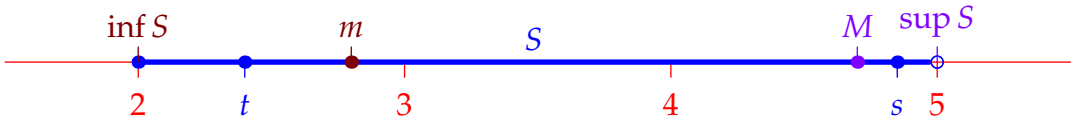


**Example 1.17.** The interval $S = [2,5)$ has $\sup S = 5$ and $\inf S = 2$ $(= \min S)$. We verify these claims: (a), (b) are the properties in the definition.

(a) Since $s \in S \iff 2 \le s < 5$, we see that 5 is indeed an upper bound and 2 a lower bound.

(b) We demonstrate the contrapositive. Suppose $M < 5$ and define[6] $s = \max\{\frac{1}{2}(M+5), 4\}$. Then $M < s < 5$ and $s \in S$. It follows that $M$ is *not* an upper bound for $S$. The least upper bound is therefore $\sup S = 5$.

For the infimum: if $m > 2$, define $t = \min\{\frac{1}{2}(m+2), 4\}$ to see that $2 < t < m$ and $t \in S$, whence $m$ is not a lower bound.




**Axiom 1.18 (Completeness of $\mathbb{R}$).** If $S \subseteq \mathbb{R}$ is non-empty and bounded above, then $\sup S$ exists (and is a real number!).

It is precisely this property that distinguishes the real numbers from the rationals.[7] Certainly every bounded set $S$ of *rational* numbers has a supremum; the issue is that $\sup S$ *need not be rational*!

By reflecting across zero (Exercise 9), we obtain the same thing for the infimum.

**Theorem 1.19 (Existence of Infima).** *If $S \subseteq \mathbb{R}$ non-empty and bounded below, then $\inf S \in \mathbb{R}$ exists.*

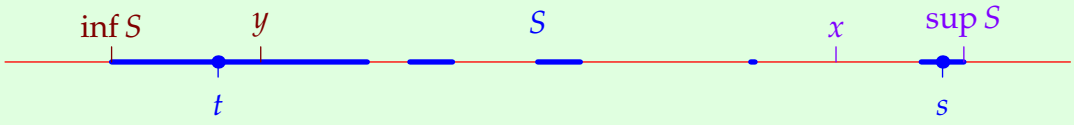
**A Useful Contrapositive** Part (b) of the Definition is plainly a biconditional: if $\sup S \le M$, then $M$ is at least as large as an upper bound and is therefore also an upper bound for $S$ (Lemma 1.14)! As in Example 1.17, one often uses the contrapositive of part (b):

> $M < \sup S$ if and only if $M$ is *not* an upper bound for $S$.

Unpacking this further using the meaning of upper bound (and substituting $x$ for $M$) we recover a useful result that will be used repeatedly.

**Lemma 1.20.** 1. *Let $S$ be bounded above. Then $x < \sup S \iff \exists s \in S$ such that $x < s$.*

2. *Let $S$ be bounded below. Then $y > \inf S \iff \exists t \in S$ such that $t < y$.*




[6] The number 4 is merely an arbitrary element to make sure $s \in S$ in case $M$ were huge and negative!

[7] More formally (the details are too much for us): if $\mathbb{F}$ is an ordered field with $0 \neq 1$ and which satisfies the completeness axiom, then $\mathbb{F}$ is isomorphic to the real numbers.

**Examples 1.21.** We state the following without proof or calculation. You should be able to justify everything using the definition, or by mirroring Example 1.17.

1. A bounded set has many possible bounds, but only one supremum or infimum.
2. If $S$ has a maximum, then $\max S = \sup S$. Similarly, if a minimum exists, then $\min S = \inf S$.
3. (Example 1.15) $S = \mathbb{Q} \cap [0, \sqrt{2})$ has $\sup S = \sqrt{2}$: this is a set of rational numbers whose supremum is not rational.
4. $S = \mathbb{Q} \cap (\pi, 4)$ has $\sup S = 4$, $\inf S = \pi$, and no maximum nor minimum.
5. $S = \{\frac{1}{n} : n \in \mathbb{N}\} = \{\ldots, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, 1\}$ has $\sup S = \max S = 1$, $\inf S = 0$, and no minimum.
6. $S = \bigcup_{n=1}^{\infty} [n, n + \frac{1}{2}) = [1, 1.5) \cup [2, 2.5) \cup [3, 3.5) \cup \cdots$ has $\inf S = 1$. It is not bounded above.
7. $S = \bigcap_{n=1}^{\infty} [\frac{1}{n}, 1 + \frac{1}{n})$ has $\inf S = 1 = \sup S$ since $S = \{1\}$.

### The Archimedean Property and the Density of the Rationals

We finish this section by discussing a crucial property related to completeness, and of the distribution of the rational numbers among the reals.

**Theorem 1.22 (Archimedean Property).** *If $b > 0$ is a real number, then $\exists n \in \mathbb{N}$ such that $n > b$.*
*More generally: $a, b > 0 \implies \exists n \in \mathbb{N}$ such that $an > b$.*

We assume nothing about $\mathbb{R}$ except that is an ordered field satisfying the completeness axiom and where $0 \neq 1$ (footnote 7). The natural numbers in this context are *defined* as the subset

$$\mathbb{N} = \{1, 1+1, 1+1+1, \ldots\} \subseteq \mathbb{R}$$

and Peano's axioms are a *theorem.*

*Proof.* Suppose the result were false. Then $\exists b > 0$ such that $n \leq b$ for all $n \in \mathbb{N}$; that is, $\mathbb{N}$ is bounded above! By completeness, $\sup \mathbb{N}$ exists, and we trivially see that

$$0 < 1 \implies \sup \mathbb{N} < \sup \mathbb{N} + 1 \implies \sup \mathbb{N} - 1 < \sup \mathbb{N}$$

By Lemma 1.20, $\exists n \in \mathbb{N}$ such that $n > \sup \mathbb{N} - 1$. But then $\sup \mathbb{N} < n + 1$ which is clearly a natural number! Thus $\sup \mathbb{N}$ is not an upper bound for $\mathbb{N}$: contradiction.
For the more general statement, simply replace $b$ with $\frac{b}{a}$. ∎

The use of completeness is *necessary*: there exist non-Archimedean ordered fields!

**Example (1.15, cont.).** The Archimedean property is precisely what is needed to justify the existence of an integer $N > -\log_{10}(\sqrt{2} - M)$.

**Corollary 1.23 (Density of $\mathbb{Q}$ in $\mathbb{R}$).** *Between any two real numbers, there exists a rational number.*

The idea is hopefully straightforward: given $a < b$, stretch the interval by an integer factor $n$ until it contains an integer $m$, before dividing by $n$ to obtain $a < \frac{m}{n} < b$. We use the Archimedean property to establish the existence of the scale factors $m, n$.

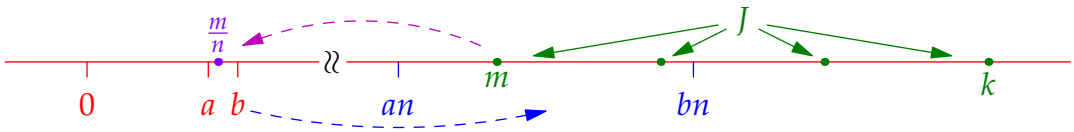
*Proof.* Suppose WLOG that $0 \leq a < b$, and apply the Archimedean property to $\frac{1}{b-a} > 0$:

$$\exists n \in \mathbb{N} \text{ such that } n > \tfrac{1}{b-a}$$

A second application (or trivially if $a = 0$) says $\exists k \in \mathbb{N}$ such that $k > an$. Now consider the set

$$J := \{j \in \mathbb{N} : an < j \leq k\}$$

and define $m = \min J$: this exists since $J$ is a finite non-empty set of natural numbers.[8]




Clearly $m > an > m - 1$, since $m = \min J$. But then $m \leq an + 1 < bn$. We conclude that

$$an < m < bn \implies a < \frac{m}{n} < b$$

■

By iterating this result we see that any interval $(a, b)$ contains *infinitely many* rational numbers. It can moreover be established that the irrational numbers are also dense in $\mathbb{R}$ (Exercise 6).

**Exercises 1.4.** *Key concepts: Suprema, Completeness (distinguishes $\mathbb{R}$), Contrapositive criterion, Archimedean property/Density of $\mathbb{Q} \subset \mathbb{R}$*

1. Decide whether each set is bounded above and/or below. If so, state its supremum and/or infimum (no working is required).

   (a) $(0, 1)$ (b) $\{2, 7\}$ (c) $\{0\}$

   (d) $\bigcup_{n=1}^{\infty} [2n, 2n+1]$ (e) $\{1 - \frac{1}{3^n} : n \in \mathbb{N}\}$ (f) $\{r \in \mathbb{Q} : r^2 < 2\}$

   (g) $\bigcup_{n=1}^{\infty} (1 - \frac{1}{n}, 1 + \frac{1}{n})$ (h) $\{\frac{1}{n} : n \in \mathbb{N} \text{ and } n \text{ is prime}\}$ (i) $\{\cos(\frac{n\pi}{3}) : n \in \mathbb{N}\}$

2. Modelling Example 1.15, *sketch* an argument that $S = \mathbb{Q} \cap (\pi, 4]$ has no minimum.
   (*Hint: let $s_n$ be $\pi$ rounded up to $n$ decimal places*)

3. Let $S$ be a non-empty, bounded subset of $\mathbb{R}$.
   (a) Prove that $\inf S \leq \sup S$.
   (b) What can you say about $S$ if $\inf S = \sup S$?

[8] This part of the argument is necessary since, in this context, we haven't established the well-ordering property of $\mathbb{N}$ (essentially Peano's fifth axiom).

4. Let $S$ and $T$ be non-empty subsets of $\mathbb{R}$ with the property that $s \leq t$ for all $s \in S$ and $t \in T$.

   (a) Prove that $S$ is bounded above and $T$ bounded below.

   (b) Prove that $\sup S \leq \inf T$.

   (c) Give an example of such sets $S, T$ where $S \cap T$ is non-empty.

   (d) Give an example of such sets $S, T$ where $S \cap T$ is empty, and $\sup S = \inf T$.

5. Prove that if $a > 0$ then there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < a < n$.

6. Let $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ be the set of *irrational* numbers. Given real numbers $a < b$, prove that there exists $x \in \mathbb{I}$ such that $a < x < b$.

   (*Hint: First show* $\{r + \sqrt{2} : r \in \mathbb{Q}\} \subseteq \mathbb{I}$)

7. Let $A, B$ be non-empty bounded subsets of $\mathbb{R}$, and let $S$ be the set of all sums

   $$S := \{a + b : a \in A, b \in B\}$$

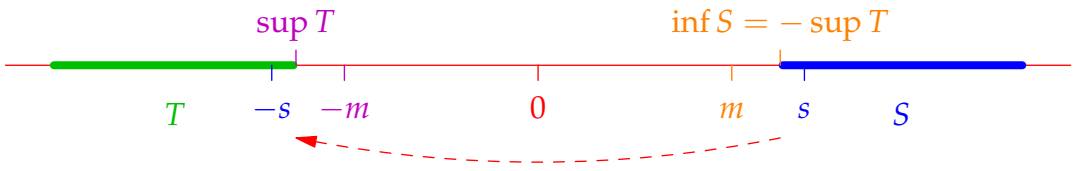
   (a) Prove that $\sup S = \sup A + \sup B$.

   (b) Prove that $\inf S = \inf A + \inf B$.

8. Show that $\sup\{r \in \mathbb{Q} : r < a\} = a$ for each $a \in \mathbb{R}$.

9. We prove Theorem 1.19 on the existence of the infimum.

   Let $S \subseteq \mathbb{R}$ be non-empty and let $m$ be a lower bound for $S$. Define $T = \{t \in \mathbb{R} : -t \in S\}$ by reflecting $S$ across zero.




   (a) Prove that $-m$ is an upper bound for $T$.

   (b) By completeness (Axiom 1.18), $\sup T$ exists. Prove that $\inf S = -\sup T$ by verifying Definition 1.16 parts 2(a) and (b).

## 1.5 The Symbols $\pm\infty$

Thus far the only subsets of the real numbers that have a supremum are those which are *non-empty* and *bounded above*. In this very short section, we introduce the $\infty$-symbol to provide all subsets of the real numbers with both a supremum and an infimum.

**Definition 1.24.** Let $S \subseteq \mathbb{R}$ be any subset. If $S$ is bounded above/below, then $\sup S / \inf S$ are as in Definition 1.16. Otherwise:

1. We write $\sup S = \infty$ if $S$ is *unbounded above*, that is

   $$\forall x \in \mathbb{R}, \exists s \in S \text{ such that } s > x$$

2. We write $\inf S = -\infty$ if $S$ is *unbounded below*,

   $$\forall y \in \mathbb{R}, \exists t \in S \text{ such that } t < y$$

3. By convention, $\sup \emptyset := -\infty$ and $\inf \emptyset := \infty$, though these will rarely be of use to us.

The symbols $\pm\infty$ have *no other meaning* (as yet); in particular, they are *not numbers*. If one is willing to abuse notation and write $x < \infty$ and $y > -\infty$ for any real numbers $x, y$, then the conclusions of Lemma 1.20 are precisely statements 1 & 2 above!

**Examples 1.25.** 1. $\sup \mathbb{R} = \sup \mathbb{Q} = \sup \mathbb{Z} = \sup \mathbb{N} = \infty$, since all are unbounded above. We also have $\inf \mathbb{R} = \inf \mathbb{Q} = \inf \mathbb{Z} = -\infty$ (recall that $\inf \mathbb{N} = \min \mathbb{N} = 1$).

2. If $a < b$, then *any* interval $[a,b]$, $(a,b)$, $[a,b)$ or $(a,b]$ has supremum $b$ and infimum $a$, even if one end is infinite. For example,

   $$S = (7, \infty) = \{x \in \mathbb{R} : x > 7\}$$

   has $\sup S = \infty$ and $\inf S = 7$.

3. Let $S = \{x \in \mathbb{R} : x^3 - 4x < 0\}$. With a little factorization, we see that

   $$x^3 - 4x = x(x-2)(x+2) < 0 \iff x < -2 \text{ or } 0 < x < 2$$

   It follows that $S = (-\infty, -2) \cup (0, 2)$, from which $\sup S = 2$ and $\inf S = -\infty$.

**Exercises 1.5.** *Key concepts:* $\pm\infty$ *are shorthands for* ***unboundedness****: they are* ***not numbers****!*

1. Give the infimum and supremum of each of the following sets:

   (a) $\{x \in \mathbb{R} : x < 0\}$ (b) $\{x \in \mathbb{R} : x^3 \leq 8\}$

   (c) $\{x^2 : x \in \mathbb{R}\}$ (d) $\{x \in \mathbb{R} : x^2 < 8\}$

2. Let $S \subseteq \mathbb{R}$ be non-empty, and let $-S = \{-s : s \in S\}$. Prove that $\inf S = -\sup(-S)$.

3. Let $S, T \subseteq \mathbb{R}$ be non-empty such that $S \subseteq T$. Prove that $\inf T \leq \inf S \leq \sup S \leq \sup T$.

4. If $\sup S < \inf S$, what can you say about $S$?

## 1.6 A Development of $\mathbb{R}$ (non-examinable)

The comment in footnote 7 constitutes a *synthetic* definition of the real numbers: there is essentially just one set with the required properties. While this might satisfy an algebra-addict, it is nice to be able to provide an explicit construction. The following approach uses so-called *Dedekind cuts.*

First one defines $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$. Use Peano's axioms and proceed as in sections 1.1 and 1.2. The operations $+, \cdot$ and $\leq$ are defined, first on $\mathbb{N}$ and then for $\mathbb{Z}$ and $\mathbb{Q}$ building on these concepts for the integers.

**Definition 1.26.** A *Dedekind cut* $\alpha^*$ is a non-empty proper subset of $\mathbb{Q}$ with the properties:

1. (Closed downwards) If $r \in \alpha^*$ and $s \in \mathbb{Q}$ with $s < r$, then $s \in \alpha^*$.
2. (No maximum) If $M$ is an upper bound for $\alpha^*$, then $M \notin \alpha^*$.

Define $\mathbb{R}$ to be the set of all Dedekind cuts!

The rough idea is that a real number $\alpha$ corresponds to the Dedekind cut $\alpha^*$ of all *rational numbers less than* $\alpha$.

**Examples 1.27.** 1. For any *rational number* $r$, the corresponding *real number* is the Dedekind cut

$$r^* = \{x \in \mathbb{Q} : x < r\}$$

For instance $4^* = \{x \in \mathbb{Q} : x < 4\}$ is the Dedekind cut definition of the *real number* 4.

2. It is a little trickier to explicitly define cuts corresponding to irrational numbers, though some are relatively straightforward. For instance the real number $\sqrt{2}$ would be the set

$$\sqrt{2}^* = \{x \in \mathbb{Q} : x < 0 \text{ or } x^2 < 2\}$$

It remains to *prove* that the set of Dedekind cuts satisfies the axioms of a complete ordered field. The full details are too much, so here is a rough overview.

- Define the ordering of Dedekind cuts via

  $$\alpha^* \leq \beta^* \iff \alpha^* \subseteq \beta^*$$

  One can now prove axioms O1–O3 and that the ordering corresponds to that of $\mathbb{Q}$.

- Define addition of cuts via

  $$\alpha^* + \beta^* := \{a + b : a \in \alpha^*, b \in \beta^*\}$$

  This suffices to prove the addition axioms and O4: a careful definition of $-\alpha^*$ is required.

- Multiplication is horrible: if $\alpha^*, \beta^* \geq 0^*$ then

  $$\alpha^*\beta^* := \{ab : a \geq 0, a \in \alpha^*, b \geq 0, b \in \beta^*\} \cup \{q \in \mathbb{Q} : q < 0\}$$

  which may be carefully extended to cover situations when $\alpha^*$ or $\beta^* < 0^*$. Once this has been done, one can then prove the multiplication axioms, the final order axiom O5, and the distributive axiom.

- The completeness axiom must also be verified, though it comes almost for free! If $A \subseteq \mathbb{R}$ (a set of Dedekind cuts), then the supremum of $A$ is simply

$$\sup A = \bigcup_{\alpha^* \in A} \alpha^*$$

Think about it...

An alternative approach to $\mathbb{R}$ using sequences of rational numbers will be given later.

**Exercises 1.6.** *Key concepts:* $\mathbb{R}$ *is unnatural and difficult to construct in a logical manner*

1. Show that if $\alpha^*, \beta^*$ are Dedekind cuts, then so is

$$\alpha^* + \beta^* = \{r_1 + r_2 : r_1 \in \alpha^*, r_2 \in \beta^*\}$$

2. Let $\alpha^*, \beta^*$ be Dedekind cuts and define the 'product':

$$\alpha^* \cdot \beta^* = \{r_1 r_2 : r_1 \in \alpha^*, r_2 \in \beta^*\}$$

   (a) Calculate some 'products' using the cuts $0^*, 1^*$ and $(-1)^*$.

   (b) Discuss why this 'product' is unsatisfactory for defining multiplication in $\mathbb{R}$.

3. We verify the Archimedean property (Theorem 1.22) using the Dedekind cut definition of $\mathbb{R}$ (it is somewhat easier since the unboundedness of $\mathbb{N}$ and $\mathbb{Q}$ are baked in).

   (a) Explain why every cut $\beta^*$ is bounded above by some rational number.
   (*Hint: if $\beta^*$ satisfies Definition 1.26 parts 1 & 2 but is unbounded above, then what is it?*)

   (b) If $\beta^* > 0^*$ is a positive cut bounded above by $\frac{p}{q}$ with $p, q \in \mathbb{N}$, show that $n := p + 1$ corresponds to a cut for which $n^* > \beta^*$.