Instructor: Leo Goldmakher

Williams College
Department of Mathematics and Statistics

MATH 350 : REAL ANALYSIS

Solution Set 5

(1) Prove that for any $x \in \mathbb{R}$ there exists $N \in \mathbb{Z}$ and $\alpha \in [0,1)$ such that $x = N + \alpha$, and that this choice of N and α are uniquely determined by x. (Recall from class that N is called the *floor* of x, denoted $\lfloor x \rfloor$, and α is called the *fractional part* of x, denoted $\{\alpha\}$. For example, $\lfloor \pi \rfloor = 3$ and $\{\pi\} = 0.1415926\ldots$)

[NOTE. *In class we proved the above statement for $x \geq 1$. You may use that result without reproving it!*]

For $x \in [0,1)$, set $N := 0$ and $\alpha := x$. Note that this choice is unique: for any $N \in \mathbb{Z}_{\text{pos}}$ we have $N \geq 1$, so $x - N < 0$; if, on the other hand, $-N \in \mathbb{Z}_{\text{pos}}$, then $-N \leq -1$ so $x - N < 0$. Given the existence and uniqueness, we may extend our definitions of floor and fractional part to all $x \geq 0$: $\lfloor x \rfloor$ and $\{x\}$ for all $x \geq 0$.

For $x < 0$, we split into two cases. If $x \in \mathbb{Z}$, set $N := x$ and $\alpha := 0$. If $x \notin \mathbb{Z}$, set

$$N := -\lfloor -x \rfloor - 1 \qquad \text{and} \qquad \alpha := x - N.$$

It's clear that $N \in \mathbb{Z}$, and we know from our work in class that $-x - \lfloor -x \rfloor \in (0,1)$. Thus $\alpha = x + \lfloor -x \rfloor + 1 \in (0,1)$.

Now we must show N and α are unique. Suppose there are two values of N that work, call them N and N', each with an associated fractional part, call them α and α'. Now we have $x = N + \alpha = N' + \alpha'$, where $N, N' \in \mathbb{Z}$ and $\alpha, \alpha' \in [0,1)$. Since N and N' are both integers, their difference is an integer. $N + \alpha = N' + \alpha' \implies N - N' = \alpha' - \alpha$, so $\alpha' - \alpha$ must be an integer. Since $\alpha' \geq 0$ and $\alpha < 1$, we know $\alpha' - \alpha > -1$. Likewise, since $\alpha' > 1$ and $\alpha \geq 0$, we know $\alpha' - \alpha < 1$. Thus $\alpha' - \alpha = 0$, meaning $\alpha' = \alpha$, which in turn means $N' = N$, so the choices of N and α are unique.

(2) In class, we proved that $\sqrt{2} \in \mathbb{R}$. Earlier, we gave a meta-analytic proof that $\sqrt{2} \notin \mathbb{Q}$. The goal of this problem is to give an analytic proof that $\sqrt{2}$ is irrational due to John Conway (1937-2020). Here and throughout, set $\mathbb{Q}_{\text{pos}} := \{\frac{a}{b} : a, b \in \mathbb{Z}_{\text{pos}}\}$; we call the elements of this set the *positive rational numbers*. Let

$$\mathcal{A} := \{m \in \mathbb{Z}_{\text{pos}} : m\sqrt{2} \in \mathbb{Z}_{\text{pos}}\}.$$

(a) Give the simplest colloquial (i.e. meta-analytic) description of the set $\mathcal{A}$ you can come up with. [*Hint: try to use the word 'denominator'.*]

It's the collection of all the positive denominators that arise when writing $\sqrt{2}$ as a fraction.

(b) Prove that if $a, b \in \mathbb{Z}_{\text{pos}}$, then there exists $c \in \mathbb{Z}_{\text{pos}} \cup \{0\}$ such that $0 \leq c < b$ and

$$\left\{\frac{a}{b}\right\} = \frac{c}{b}.$$

[*In the first line, $\{0\}$ denotes the set with the single element 0; in the displayed equation, $\left\{\frac{a}{b}\right\}$ denotes the fractional part of $\frac{a}{b}$.*]

From class, we know there exists $N \in \mathbb{Z}_{\text{pos}} \cup \{0\}$ such that

$$\left\{\frac{a}{b}\right\} = \frac{a}{b} - N = \frac{a - bN}{b}.$$

On the other hand, we know $0 \leq \{\frac{a}{b}\} < 1$, whence

$$0 \leq a - bN < b.$$

Letting $c := a - bN$ concludes the proof. □

(c) Suppose $n \in \mathcal{A}$. Prove that there must exist $k \in \mathbb{Z}_{\text{pos}}$ such that $\sqrt{2} = \frac{k}{n} = \frac{2n}{k}$.

By definition of $\mathcal{A}$, if $n \in \mathcal{A}$ then it's the denominator of some fractional representation of $\sqrt{2}$, i.e. there's some $k \in \mathbb{Z}_{\text{pos}}$ such that $\sqrt{2} = \frac{k}{n}$. This implies $2n^2 = k^2$, whence $\frac{k}{n} = \frac{2n}{k}$.

(d) Keeping the notation as above, prove that $\exists k', n' \in \mathbb{Z}$ such that $0 < k' < k$, $0 < n' < n$, and $\frac{n'}{n} = \frac{k'}{k}$.

First, observe

Lemma. $\{\sqrt{2}\} \neq 0$.

By (c), it follows that $0 \neq \{\frac{k}{n}\} = \{\frac{2n}{k}\}$. From (b) we have

$$(*) \qquad 0 \neq \left\{\frac{k}{n}\right\} = \frac{n'}{n} \qquad \text{and} \qquad 0 \neq \left\{\frac{2n}{k}\right\} = \frac{k'}{k}$$

for some $k' \in [0, k)$ and $n' \in [0, n)$. From $(*)$, we see $k' \neq 0$ and $n' \neq 0$, which concludes the proof. □

Proof of Lemma. By definition, $\sqrt{2} > 0$, so if $\sqrt{2} \leq 1$ then $2 \leq 1$, which is false. It follows that $\sqrt{2} > 1$. Multiplying both sides by $\sqrt{2}$ implies $\sqrt{2} < 2$. In sum,

$$1 < \sqrt{2} < 2.$$

By Lemma 6.9, $\sqrt{2} \notin \mathbb{Z}_{\text{pos}}$. The claim immediately follows. □

(e) Keeping the notation as above, prove that $n' \in \mathcal{A}$.

Since $\frac{n'}{n} = \frac{k'}{k}$ and neither of n' or k' are zero, we deduce that

$$\sqrt{2} = \frac{k}{n} = \frac{k'}{n'}.$$

Thus, by definition, $n' \in \mathcal{A}$.

(f) Prove that $\mathcal{A} = \emptyset$. Why does this imply that $\sqrt{2} \notin \mathbb{Q}_{\text{pos}}$?

Putting together all our above work, we deduce whenever a positive integer $n \in \mathcal{A}$, there exists some positive integer $n' < n$ that's also in $\mathcal{A}$. This implies $\mathcal{A}$ has no least element. But $\mathbb{Z}_{\text{pos}}$ is well-ordered, whence $\mathcal{A}$ must be empty. This means there's no way to write $\sqrt{2}$ as a fraction, since otherwise the denominator of that fraction would be an element of $\mathcal{A}$.

(3) (Meta-analytic) Let $\mathbb{Z}[x]$ denote the set of all polynomials with integer coefficients, and consider the set

$$\mathcal{F} := \left\{\frac{f(x)}{g(x)} : f, g \in \mathbb{Z}[x] \text{ s.t. } g \text{ isn't the constant 0 function}\right\}.$$

We'll define $h \in \mathcal{F}$ to be *positive* iff $h(x) > 0$ for all large $x \in \mathbb{R}$. Prove that $\mathcal{F}$ is an ordered field, i.e. satisfies (A1)-(A12), but that it fails to satisfy the Archimedean Property. This demonstrates that the Archimedean Property cannot be deduced from (A1)-(A12) alone!

By properties of polynomials (namely they're commutative, associative, and etc.) we get that $\mathcal{F}$ is closed under addition/multiplication and abides by commutativity and associativity. The additive identity is 0 and the multiplicative identity is 1. The additive inverse of $\frac{f(x)}{g(x)}$ is $\frac{-f(x)}{g(x)}$. The multiplicative inverse of $\frac{f(x)}{g(x)}$ is $\frac{g(x)}{f(x)}$. Regular properties of polynomials also ensures distributive laws.

Thus, it suffices to show (A12). We're given a potential set of positives:

$$\mathbb{P} = \{h \in \mathcal{F} \ : \ h(x) > 0 \text{ for all large } x \in \mathbb{R}\}.$$

Given $h, m \in \mathbb{P}$; then $h(x), m(x)$ are greater than 0 for all sufficiently large x. Then definitely the sum $h(x) + m(x)$ is also greater than 0 for all sufficiently large x (if $h(x) > 0$ for all $x > C$ and $m(x) > 0$ for all $x > C'$, then $h(x) + m(x) > 0$ for all $x > \max\{C, C'\}$). The same is true of the product $h(x)m(x)$, meaning that $\mathbb{P}$ is closed under addition/multiplication.

We now need to show trichotomy. Pick $f \in \mathcal{F}$. If $f = 0$, then $f \notin \mathbb{P}$ and $-f \notin \mathbb{P}$. Otherwise, exactly one of $f \in \mathbb{P}$ or $-f \in \mathbb{P}$ (the highest degree dominates so if the coefficient of the highest degree is positive then for all sufficiently large x the function is positive, and if it's negative then for all sufficiently large x the function is negative). We deduce trichotomy, and thus, that $\mathcal{F}$ is an ordered field.

To show that $\mathcal{F}$ doesn't satisfy the Archimedean Property, we need to show there's some $f \in \mathcal{F}$ s.t. $f - n > 0$ for every $n \in \mathbb{Z}_{\text{pos}}$, i.e. that the integers are *not* arbitrarily large. There are many such choices of f! For example, $f(x) = x$ satisfies this, since for any positive integer n, the polynomial $x - n \in \mathbb{P}$. It follows that x is larger than every $n \in \mathbb{Z}_{\text{pos}}$.

(4) (Meta-analytic) Textbook problem 7.10: Prove that no equilateral triangle in the plane can have all vertices with rational coordinates.

PROOF. Suppose there exists an equilateral triangle with all three vertices having rational coordinates. After translating by a rational amount, we may assume that one of the vertices of the triangle is at the origin. Denote the other two vertices (a, b) and (c, d), and observe that $|(a, b)| = |(c, d)|$. We'll compute the area of the triangle in two different ways and derive a contradiction.

First, the triangle is half of the image of the unit square under the linear map $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, so its area is $\frac{1}{2}|ad - bc|$. On the other hand, its area is

$$\frac{1}{2}|(a, b)| \cdot |(c, d)| \sin \frac{\pi}{3} = \frac{\sqrt{3}}{4}|(a, b)|^2 = \frac{\sqrt{3}}{4}(a^2 + b^2).$$

(Note that $a^2 + b^2 \neq 0$, else this would be a degenerate triangle.) Comparing these two areas and simplifying yields

$$\sqrt{3} = \frac{2|ad - bc|}{a^2 + b^2}.$$

Since the right hand side is rational while the hand side is not (see Lemma below), we've arrived at a contradiction.

continued on next page...

Lemma. $\sqrt{3} \notin \mathbb{Q}$.

Proof. We adapt Conway's proof. Let

$$\mathcal{A} := \{b \in \mathbb{Z}_{\text{pos}} : b\sqrt{3} \in \mathbb{Z}\}.$$

We'll show that if $n \in \mathcal{A}$ then there exists $n' \in \mathcal{A} \cap (0, n)$. But this implies that $\mathcal{A}$ has no least element, which is only possible if $\mathcal{A} = \emptyset$.

Suppose $n \in \mathcal{A}$. Then there exists $k \in \mathbb{Z}$ such that $\sqrt{3} = \frac{k}{n}$. Squaring and rearranging implies

$$\sqrt{3} = \frac{k}{n} = \frac{3n}{k}.$$

Taking fractional parts of both sides (and noting that $1 < \sqrt{3} < 2$) we find that

$$0 \neq \left\{\frac{k}{n}\right\} = \left\{\frac{3n}{k}\right\}.$$

Thus, there exist integers $n' \in (0, n)$ and $k' \in (0, k)$ such that $\frac{n'}{n} = \frac{k'}{k}$. But then $\frac{k'}{n'} = \frac{k}{n} = \sqrt{3}$, whence $n' \in \mathcal{A}$. This concludes the proof. □

(5) (Meta-analytic) Use induction to prove that $2^{2^n} - 1$ has at least n distinct prime factors.

[*Hint. If two integers a and b are both multiples of n, then so is $a - b$.*]

We have $2^{2^n} - 1 = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1)$. By induction, $2^{2^{n-1}} - 1$ has at least $n - 1$ distinct prime factors. Pick any prime factor p of $2^{2^{n-1}} + 1$ (it must have at least one); observe that $p \neq 2$. If p were also a factor of $2^{2^{n-1}} - 1$, then it would be a factor of $(2^{2^{n-1}} + 1) - (2^{2^{n-1}} - 1) = 2$, which is impossible. Thus p cannot be a factor of $2^{2^{n-1}} - 1$, whence $2^{2^n} - 1$ must have at least n prime factors.