NOTES ABOUT NATURAL NUMBERS

MAT157, FALL 2020–20201. YAEL KARSHON

These notes[1] supplement Spivak's Chapter 2. Please let me know if you find a mistake or if you would like a further explanation of any part of the notes.

In this handout I am skipping some proofs and giving some other proofs. It would be useful for you to work out some of the proofs that I am skipping and to fill the details of the proofs that I am giving, (and it can be fun!), but I would like you to give a higher priority to the stuff that is in the textbook and on the problems set. Specifically, you need to be able to use induction to prove statements about natural numbers, as in the examples in Spivak's book.

The set of natural numbers is

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

Note that we start with 1. (Some mathematicians start with 0.) Thus,

- *1 is a natural number.*
- *If n is a natural number, then $n+1$ is also a natural number.*

Here is the **principle of mathematical induction**:

- *Let $A \subseteq \mathbb{N}$ be a set of natural numbers. Suppose that*
  - *A contains the number 1; and*
  - *For any natural number n, if A contains n, then A also contains $n+1$.*

  Then A is the set of all natural numbers.

These properties of natural numbers are consequences of the definition of the set of natural numbers. (The set of natural numbers is defined to be the intersection of all the sets X of real numbers that have the following property: X contains 1, and, for any real number x, if $x \in X$ then $x+1 \in X$.) Some of you would find it satisfying to understand this definition and how it implies the above three properties of the natural numbers. All of you need to be able to use the principle of induction, in particular, to prove things by induction.

Here are some simple properties of natural numbers that you can prove by induction on n.

- *For every natural number n, $1 \leq n$.*
- *For every natural number n, either $n = 1$, or there exists a natural number k such that $n = k + 1$.*
- *For every natural number n, there is no natural number x such that $n - 1 < x < n$.*
- *If m and n are natural numbers, so is $m + n$.*
- *If m and n are natural numbers, so is mn.*

[1] Version: March 9, 2021

- *Let m and n be natural numbers. If $n > m$, then there exists a natural number k such that $m + k = n$.*

Here is a theorem that I like, whose proof relies on the least upper bound axiom.

Theorem (Archimedean property of the real numbers)**.** *The set $\mathbb{N}$ of natural numbers is not bounded from above.*

Proof. Suppose $\mathbb{N}$ is bounded from above. Let $\alpha := \sup \mathbb{N}$. Then $n \leq \alpha$ for all $n \in \mathbb{N}$. Applying this to natural numbers of the form $n = m + 1$, we obtain that $m + 1 \leq \alpha$ for all $m \in \mathbb{N}$. This further implies that $m \leq \alpha - 1$ for all $m \in \mathbb{N}$. So $\alpha - 1$ is also an upper bound for $\mathbb{N}$, contradicting the fact that α is the *least* upper bound. $\square$

Later in the year, we will encounter a system of "numbers" that satisfies the arithmetic axioms and the order axioms (i.e. it is an ordered field) but that does not have the Archimedean property. (Such a system cannot satisfy the least upper bound axiom. Do you see why?)

Exercise: For every positive number $\epsilon > 0$ there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \epsilon$.

Here is the **well ordering principle**:

> *Every non-empty set of natural numbers has a smallest element.*

The well-ordering principle says that, given a set X of natural numbers, if X is nonempty then X has a smallest element. Equivalently: if X does not have a smallest element, then X is empty.

Proof of the well ordering principle. Let X be a set of natural numbers that does not have a smallest element. We would like to prove that X is empty. We will do this by proving by induction that, for any $n \in \mathbb{N}$, the set X does not contain any natural numbers $\leq n$.

Base case, n=1:
The only natural number ≤ 1 is 1, so we need to prove that X does not contain 1. Indeed, otherwise 1 would be a smallest element of X.

Inductive step, from n to $n + 1$:
Assume that X does not contain any natural numbers $\leq n$. (This is the "induction hypothesis".) We would like to prove that X does not contain any natural numbers $\leq n + 1$. The only natural number that is $\leq n + 1$ and $\not\leq n$ is $n + 1$, so we need to prove that X does not contain $n + 1$. Indeed, otherwise $n + 1$ would be a smallest element of X. $\square$

The set of **integers** is

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

It is equal to the set of differences of natural numbers: $\mathbb{Z} = \{a - b \mid a, b \in \mathbb{N}\}$. Note that $a - b = \hat{a} - \hat{b}$ if and only if $a + \hat{b} = b + \hat{a}$.

- *Every positive integer is a natural number.*

The set of **rational numbers** is

$$\mathbb{Q} = \left\{ \frac{p}{q} \;\middle|\; p \in \mathbb{Z},\ q \in \mathbb{N} \right\}.$$

Note that $\dfrac{p}{q} = \dfrac{\hat{p}}{\hat{q}}$ if and only if $p\hat{q} = q\hat{p}$.

The set of **irrational numbers** is $\mathbb{R} \smallsetminus \mathbb{Q}$, meaning $\{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$.

Note: 0 and 1 are rational. If x and y are rational, so are $x+y$ and xy. If x is rational, so is $-x$, and so is $\dfrac{1}{x}$ if $x \neq 0$. The rational numbers satisfy the arithmetic axioms and the order axioms (so they are an ordered field) but not the least upper bound axiom.

Examples of irrational numbers: 2π, e, $\sqrt{2}$.

(Warning: we have not formally defined 2π nor e. We define $\sqrt{2}$ to be the positive number x such that $x^2 = 2$. The fact that such a number, if exists, is unique, is an easy consequence of the axioms for the real numbers, which does not require the least upper bound axiom. The fact that such a number exists is not trivial; it requires the least upper bound axiom. The fact that such a number is irrational has many proofs and is a special case of the theorem further below.)

Spivak's proof that $\sqrt{2}$ is irrational relies on the following theorem.

Theorem. *Let x be a rational number. Then $x = \frac{p}{q}$ for some $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ that are not both even.*

Proof. We need to prove that there exist $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ that are not both even and such that $x = \frac{p}{q}$. Consider the set of denominators of x:

$$\{q \in \mathbb{N} \mid x = \frac{p}{q} \text{ for some } p \in \mathbb{Z}\}.$$

Because x is rational, this set is non-empty. By the well-ordering principle, this set has a smallest element, say, q_0. Because q_0 is in this set, there exists $p_0 \in \mathbb{Z}$ such that $x = \frac{p_0}{q_0}$.

We claim that p_0 and q_0 are not both even. Seeking a contradiction, assume that p_0 and q_0 are both even. This means that $p_0 = 2k$ and $q_0 = 2l$ for some integers k and l. Because q_0 is positive, so is l. So l is a natural number. So

$$x = \frac{p_0}{q_0} = \frac{2k}{2l} = \frac{k}{l}.$$

So l is in the set of denominators of x. Since q_0 is the smallest element of the set of denominators, $q_0 \leq l$. This contradicts the fact that $q_0 = 2l$. □

Theorem. *Let n be a natural number that is not the square of any natural number. Then $\sqrt{n}$ is irrational (i.e., there is no rational number whose square is n).*

If you are struggling with the material, please skip this proof and focus on your problem set.

Proof. Fix any natural number n. Assume that n is the square of a rational number. We would like to prove that n is the square of a natural number.

Consider the set of "denominators of $\sqrt{n}$",

$$\{q \in \mathbb{N} \mid \text{ there exists } p \in \mathbb{N} \text{ such that } \left(\frac{p}{q}\right)^2 = n \ \}.$$

Because $\sqrt{n}$ is rational, this set of denominators is non-empty. By the well-ordering principle, the set has a smallest element. We will show that this smallest element cannot be greater than 1. Thus, the smallest element must be 1, so 1 is in the set of denominators, which implies that n is the square of some natural number p.

We need show that, given any expression of $\sqrt{n}$ as a quotient of natural numbers, $\sqrt{n} = \dfrac{p}{q}$, if $q > 1$ then we can find another such expression, $\sqrt{n} = \dfrac{\hat{p}}{\hat{q}}$, with a smaller denominator.

The rest of the proof is not intuitive, but you can still try to follow it. (It's taken from Dedekind's article "continuity and irrational numbers", from around 1860, where he also proposed a construction of the real numbers through what we now call *Dedekind cuts.*)

Suppose now that $p, q \in \mathbb{N}$ and $\left(\dfrac{p}{q}\right)^2 = n$. Let k be the natural number such that

$$k^2 \leq n < (k+1)^2.$$

(The well ordering principle implies that there is a smallest natural number k that satisfies $n < (k+1)^2$; such a k will also satisfy $k^2 \leq n$.)

Multiplying these inequalities by q^2 and substituting $p = nq^2$, we obtain $k^2q^2 < p^2 < (k+1)^2q^2$. Since kq, p, and $(k+1)q$ are positive, this further implies that

$$kq < p < (k+1)q.$$

Let $\hat{q} = p - kq$. Then $\hat{q}$ is a natural number, and it is strictly smaller than q. (Can you see why?) To complete our argument, we will show that $\hat{q}$ is in the set of denominators.

We calculate: $n\hat{q}^2 = n(p-kq)^2 = np^2 - 2npkq + nk^2q^2 = n^2q^2 - 2npkq + k^2p^2 = (nq-kp)^2$, where in the third equality we substituted $p^2 = nq^2$ in the first and third summands. So $\sqrt{n}$ is equal to $\dfrac{|nq-kp|}{\hat{q}}$, a quotient of two integers with denominator $< q$, as required. $\square$