BASIC PROPERTIES OF NUMBERS

AUGUST 28, 2017

1. Natural Numbers

First we have the *natural numbers* or *counting numbers*, usually denoted by the letter $\mathbb{N}$. These are just the collection $\{1, 2, 3, \ldots\}$. These have the following basic properties.

(1) **Operations:** Natural numbers have two operations, addition usually denoted by the symbol $+$ and multiplication usually written by the symbol $\cdot$ (or $\times$ or just writing the numbers next to each other).
(2) **Closure**: We may add two natural numbers to get a natural number. Similarly we can multiply two natural numbers to get a natural number.
(3) **Identity:** There exists a special element written 1 and called *one* such that $a \cdot 1 = a$ for all $a \in \mathbb{N}$.
(4) **Commutativity**: $a + b = b + a$ and $ab = ba$ for all natural numbers a, b.
(5) **Associativity**: $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$ for all natural numbers $a, b.c$.
(6) **Distributivity**: $a(b + c) = ab + ac$ for all natural numbers a, b, c.
(7) **Cancellation** If $a + c = b + c$, then $a = b$. If $ac = bc$, then $a = b$.
(8) **Notation**: In this notation, we have $2 = 1 + 1$, $3 = 2 + 1$ etc. and all these are different.
(9) **Description** If $a \in \mathbb{N}$ then either $a = 1$ or there exists a $b \in \mathbb{N}$ such that $a = b + 1$.
(10) **Ordering**: We have an *ordering* as follows. We say that for two natural numbers a, b, $a > b$, read as *a is greater than b* if there exists a natural number k so that $a = b + k$. Thus, clearly if $a > b$ and $b > c$, then $a > c$. We also write $a \geq b$ to mean either $a = b$ or $a > b$. Similarly, we have $a \leq b$ to mean $b \geq a$ etc.

(11) **Principle of mathematical Induction**: Any non-empty (important assumption) collection of natural numbers has a minimal element. That is, if S is such a collection, there exists a natural number a in S so that for any number b in S, $b \geq a$.

2. Integers

There is a larger collection, called the integers and denoted by $\mathbb{Z}$.

(1) **Operations:** The set of integers has addition and multiplication as above, extending the operations on $\mathbb{N}$. Extending here means, if $a, b \in \mathbb{N}$, we get the same number if you add them in $\mathbb{N}$ or $\mathbb{Z}$. Similarly, for multiplication.
(2) **Zero:** Integers have another special element, denoted by $0 \notin \mathbb{N}$, called *zero* such that $a + 0 = a$ for all $a \in \mathbb{Z}$.
(3) **Additive Inverse:** For any $a \in \mathbb{Z}$, there exists an integer denoted by $-a$ such that $a + (-a) = 0$, called the additive inverse of a. If $a, b \in \mathbb{Z}$, we write $a + (-b)$ as $a - b$ for brevity.
(4) **Other properties:** These operations of addition and multiplication satisfy the above properties of closure, commutativity, associativity, distributivity and ordering. It also satisfies cancellation for addition, but for multiplication only if $c \neq 0$ in the above notation. Be careful that we still say $a > b$ only if $a = b + k$ for some $k \in \mathbb{N}$, not $k \in \mathbb{Z}$.
(5) **Description:** Any integer a has the property that either $a \in \mathbb{N}$ or $a = 0$ or $-a \in \mathbb{N}$, all these being mutually exclusive.
(6) **Absolute value:** We have the absolute value of an integer, denoted by $|\cdot|$. If $a \in \mathbb{N}$, $|a| = a$, $|0| = 0$ and if $-a \in \mathbb{N}$, we have $|a| = -a$. A natural number is also called a *positive integer* and an integer which is either a natural number or zero is called a *non-negative integer*. If $-a \in \mathbb{N}$, we call a a *negative integer*. It is clear that $a > 0$ if and only if it is a positive integer. Similarly, negative and zero.

3. Rational Numbers

There is yet a larger set called the rational numbers, denoted by $\mathbb{Q}$.

(1) **Operations:** This too has compatible operations of addition and multiplication satisfying all the properties similar to the ones above.
(2) **Multiplicative Inverse:** If $0 \neq a \in \mathbb{Q}$, there exists an element denoted by $a^{-1} \in \mathbb{Q}$ (or $\frac{1}{a}$) such that $a \cdot a^{-1} = 1$.
(3) **Description:** Given $a \in \mathbb{Q}$, there exists a $0 \neq b \in \mathbb{Z}$ such that $ab \in \mathbb{Z}$. (Caution: This b is not unique.) Thus, we can

write $a = \frac{ab}{b}$ and note that $ab, b \in \mathbb{Z}$ and $b \neq 0$. Given two representations of $r \in \mathbb{Q}$ as $r = m/n$, $r = p/q$ with $m, n, p, q \in \mathbb{Z}$ and $n \neq 0, q \neq 0$, we have $mq = np$.

(4) **Absolute value:** If r is a rational number, it has three possibilities as above: $r = 0$ or $r = m/n$ with $m, n > 0$ or $r = m/n$ with $m < 0, n > 0$. The second type we call positive, last one negative. We say for $r, s \in \mathbb{Q}$, $r > s$ to mean $r - s$ is positive. Similarly $r \geq s$, if $r - s$ is either positive or zero. We also have the absolute value, $|r| = r$ if $r \geq 0$ and $|r| = -r$ if $r < 0$.

4. Real Numbers

Finally, we deal with hardest part, the set of real numbers denoted by $\mathbb{R}$ which contains $\mathbb{Q}$.

(1) **Operations:** It has addition, multiplication, subtraction and division as in the case of rationals, extending those operations, with all the usual properties of associativity etc. All the real numbers again can be divided into positive, zero or negative numbers (mutually exclusive). It has an absolute value function. A real number $x > 0$ is same as saying there exists a natural number N such that $x \geq \frac{1}{N}$.
(2) **Description:** Given any real number r and a natural number n, there exists a rational number q such that $|r - q| < \frac{1}{n}$.
(3) **Least upper bound:** This is the most important property of real numbers, which is not available for rational numbers. Given a non-empty subset $S \subset \mathbb{R}$, we say $M \in \mathbb{R}$ is an *upper bound* for S if $s \leq M$ for all $s \in S$. We say, M is the *least upper bound* often shortened to *lub*, if M is an upper bound for S and if $N < M$, then N is not an upper bound for S. The main property of real numbers is, if a non-empty subset $S \subset \mathbb{R}$ has an upper bound, then it has a lub.

Notice that the important properties of real numbers are written in terms of inequalities, so it is not surprising that many proofs will use inequalities. For this reason, the following notation is commonly used. **Notation:** Assume we have open statements $P(n), n \in \mathbb{N}$. If $P(n)$ is true for all $n \geq N$ for some $N \in \mathbb{N}$, we write $P(n)$ is true for $n \gg 0$.

One immediate consequence of the notation is,

Lemma 1. *If $P(n), Q(n)$ are open statements with $n \in \mathbb{N}$ and $P(n), Q(n)$ are true for $n \gg 0$, then $P(n) \wedge Q(n)$ is true for $n \gg 0$.*

Proof. The hypothesis says that there exists $N_1, N_2 \in \mathbb{N}$ such that $P(n)$ is true for all $n \geq N_1$, $Q(n)$ is true for all $n \geq N_2$. Let $N \in \mathbb{N}$ such that $N \geq N_1$, $N \geq N_2$ (can you see why such an N exists?). Then it is clear that $P(n) \wedge Q(n)$ is true for all $n \geq N$. $\square$

Lemma 2. *Let $x, y \in \mathbb{R}$ and assume that $x > 0$. Then for $n \gg 0$, $y < nx$.*

Proof. Since $x > 0$, we have $x \geq \frac{1}{N}$ for some $N \in \mathbb{N}$. So, $\frac{n}{N} \leq nx$ for all $n \in \mathbb{N}$. So, if we can show $y < \frac{n}{N}$ for $n \gg 0$, we would be done. From the description above, we see that $y < z$ for some $z \in \mathbb{Q}$. So, it suffices to show that $z < \frac{n}{N}$ for $n \gg 0$. Writing $z = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $b > 0$, one can easily see that $z < \frac{n}{N}$ for all $n > |a|N$. $\square$

We use the above properties to show that there exists a real number whose square is 2. We have seen in class that there is no such rational number.

Theorem 1. *There exists a real number whose square is 2.*

Proof. Let $S = \{x \in \mathbb{R} | x^2 \leq 2\}$. First we show that $S \neq \emptyset$. This is obvious, since $1 \in S$, because $1^2 = 1 \leq 2$. Next we show that S is bounded above, by showing that if $x \in S$, then $x \leq 2$. We prove this by proving the contrapositive, which is the statement that if $x > 2$, then $x \notin S$. But $x \notin S$ just means $x^2 > 2$. If $x > 2$, we have $x^2 > 4 > 2$ and so, we have proved the contrapositive.

Thus, we can appeal to the least upper bound property for S and let $\alpha \in \mathbb{R}$ be the least upper bound of S. Next we will show that $\alpha^2 = 2$, which will prove our theorem.

Again, we prove this by contradiction. So assume that $\alpha^2 \neq 2$. Then either $\alpha^2 > 2$ or $\alpha^2 < 2$. We will treat these cases separately.
Case 1: $\alpha^2 > 2$.

Then $\alpha^2 = 2 + a$ where $a > 0$. Since α is the lub for S, for any natural number n, $b_n = \alpha - \frac{1}{n}$ is not an upper bound of S. That means, there exists an $x \in S$ with $b_n < x$. Since $\alpha > 1$, $b_n > 0$ and so, $b_n^2 < x^2 \leq 2$. Writing this out, we have,

$$\alpha^2 - 2\frac{\alpha}{n} + \frac{1}{n^2} < 2.$$

Using $\alpha^2 = 2 + a$, we get,

$$a - 2\frac{\alpha}{n} + \frac{1}{n^2} < 0,$$

which in turn implies

$$a < 2\frac{\alpha}{n} - \frac{1}{n^2} < 2\frac{\alpha}{n}. \tag{1}$$

By lemma 2 above, we have by taking $y = 2\alpha, x = a$, that $2\alpha < na$ for $n \gg 0$. Putting this together with equation 1, we get,

$$a < 2\frac{\alpha}{n} < a,$$

for $n \gg 0$. This is impossible, since a can not be strictly less than a. This contradiction proves that α^2 can not be greater than 2. An identical argument will show that α^2 can not be less than 2 and that will prove that $\alpha^2 = 2$.

□