2. Axioms or real numbers

The shortest way to introduce real numbers is by giving a list of axioms. In fact, it is possible to give a one sentence definition:

Definition. $\mathbb{R}$ (real numbers) is an ordered field which has the least upper bound property (LUB property).

It takes a bit more work to explain what this definition actually means. First we will define what a field is

Definition. A <u>field</u> is a set F with 2 binary operations, called addition (denoted by $+$) and multiplication (denoted by $\cdot$) satisfying the following axioms:

(A0) $x, y \in F \Rightarrow x + y \in F$
(A1) $x + y = y + x \ \forall\ x, y \in F$
(A2) $x + (y + z) = (x + y) + z \ \forall\ x, y, z \in F$
(A3) $\exists 0 \in F$ such that $x + 0 = x \ \forall\ x \in F$
(A4) $\forall x \in F \ \exists\ -x \in F$ such that $x + (-x) = 0$
(M0) $x, y \in F \Rightarrow xy \in F$
(M1) $xy = yx \ \forall\ x, y \in F$
(M2) $x(yz) = (xy)z \ \forall\ x, y, z \in F$
(A3) $\exists 1 \in F$ such that $x \cdot 1 = x \ \forall\ x \in F$
(A4) $\forall x \in F$ with $x \neq 0 \ \exists\ x^{-1} \in F$ such that $x \cdot x^{-1} = 1$
(D) $x(y + z) = xy + xz \ \forall\ x, y, z \in F$
(O) $0 \neq 1$

Remark: 1. Just by saying that $+$ and $\cdot$ are binary operations on F one can actually implies that axioms (A0) and (M0) must hold, so in principle those axioms need not appear on the above list. However, it is a good idea to include them since when you want to prove that a certain set is a field with respect to certain operations, those properties have to be checked.

2. There is a "strange" algebraic object with 2 binary operations which has just one element, which happens to be both 0 and 1. This object satisfies all of the above axioms except (O). The only point of the axiom (O) is to prevent that object from being considered a field (which happens to be convenient for many different reasons).

The familiar examples of fields include $\mathbb{Q}$ (rationals), $\mathbb{R}$ (reals), $\mathbb{C}$ (complex numbers) and $\mathbb{Z}_p$ (congruence classes mod p where p is a fixed prime).

Integers ($\mathbb{Z}$) is not a field since not all nonzero elements (in fact, very few elements) have multiplicative inverses.

Next we define the notion of an ordered set.

Definition. An ordered set is a set S with a binary relation $<$ satisfying the following axioms:

(O1) $\forall\, x, y \in S$ exactly one of the following holds: $x < y$, $y < x$ or $x = y$

(O2) Transitivity: if $x < y$ and $y < z$, then $x < z$

In an ordered set we write $x > y \iff y < x$. Also we write $x \leq y \iff x < y$ or $x = y$.

Example 2.1. *(1) $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ are ordered sets with $<$ in the usual sense*

(2) $\mathbb{C}$ is an ordered set with respect to the lexicographic order $<$ defined as follows: $a + bi < c + di \iff a < c$ or ($a = c$ and $b < d$)

Definition. An ordered field is a set F which is both a field and an ordered set and satisfies the following additional axioms:

(OF1) If $x, y \in F$ and $x < y$, then $x + z < y + z$ for all $z \in F$

(OF2) If $x > 0$ and $y > 0$, then $xy > 0$

Example 2.2. *(1) $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields (with the usual $<$)*

(2) $\mathbb{C}$ with the lexicographic order is not an ordered field since (OF2) fails: let $x = y = i$. Then $x = 0 + 1 \cdot i > 0$ and $y > 0$, but $xy = -1 < 0$.

A more general argument shows that $\mathbb{C}$ is not an ordered field with respect to ANY order $<$ (see HW#1).

2.1. **Least upper bound property.**

Definition. Let $(X, <)$ be an ordered set, let S be a subset of X, and let $M \in X$. We say that

(a) M is an upper bound for S if $s \leq M\ \forall s \in S$

(b) M is a least upper bound (LUB) for S if
  (i) M is an upper bound for S
  (ii) if x is any upper bound for S, then $M \leq x$

  It is not hard to show that if LUB of S exists, then it is unique. LUB of S is frequently called the supremum of S and denoted by $\sup(S)$.

(c) S is called bounded above if it has (at least one) upper bound

(d) X has the least upper bound (LUB) property if for every $S \subseteq X$ which is non-empty and bounded above, $\sup(S)$ exists (in X).

Example 2.3. *(1)* $\mathbb{R}$ *has the LUB property*

(2) $\mathbb{Z}$ *also has the LUB property. In fact, it even has a stronger property: if* $S \subseteq \mathbb{Z}$ *is bounded, then* $\max(S)$ *exists.*

(3) $\mathbb{Q}$ *does not have the LUB property.*

To prove (3) we need to exhibit a subset S of $\mathbb{Q}$ such that S is non-empty and bounded above, but does not have a supremum (in $\mathbb{Q}$).

Claim 2.4 (HW#1.6)**.** *The set* $S = \{x \in \mathbb{Q} : x < \sqrt{2}\} = \{x \in \mathbb{Q} : x \leq 0 \text{ or } x^2 < 2\}$ *has both properties.*

To be completed.