Notes for 445.255 Principles of Mathematics

The Real Numbers

One approach to the real numbers is "constructive". The natural numbers (positive integers) can be defined in terms of elementary set theory. Then we can construct the integers as suitable equivalence classes of natural numbers and the rational numbers as equivalence classes of integers.

The resulting system of numbers corresponds to points on a line but it is easily seem that there are points on the line which do not correspond to any of our rational numbers. For example there is no rational x for which $x^2 = 2$.

> Suppose the rational number p/q is a solution (where p, q are integers, $q \neq 0$ and the fraction is in its lowest terms). Then $p^2 = 2q^2$ and hence p is even
> ($p = 2m+1$ i.e. odd $\implies$ p^2 odd). Let $p = 2r$. Then we get $2r^2 = q^2$. So q is also even, contradicting the assumption that the fraction p/q was in its lowest terms. Hence p/q is not a solution.

To ensure that all points on the line correspond to numbers we must enlarge the number system even further. In this enlarged system the equation $x^2 = 2$ *does* have a solution, namely the real number $\sqrt{2}$. But other real numbers such as π and e do not arise as the solutions of such (algebraic) equations.

The construction of the real numbers from the rationals can be achieved by again considering appropriate equivalence classes. However the details are rather cumbersome and we prefer to define the real numbers directly as objects satisfying certain axioms. Subsets of the real numbers will then be identified with the natural and rational numbers respectively.

Algebraic (field) Properties of $\mathbb{R}$

A field is a set S such that S and $S - \{0\}$ is a commutative group with respect to two operations $+$ and $*$ and $*$ is distributive over $+$.

We assume that $\mathbb{R}$ is closed under two binary operations

$$(x, y) \to x + y \qquad (x, y) \to xy$$

(called addition and multiplication respectively) which satisfy the following properties:

F1	$x + y = y + x$	$xy = yx$	(commutative laws)
F2	$x + (y + z) = (x + y) + z$	$x(yz) = (xy)z$	(associative laws)
F3	$x(y + z) = (xy + xz)$		(distributive law)
F4	There are two distinct elements of $\mathbb{R}$, denoted by 0 and 1, such that for every		

x in $\mathbb{R}$ we have $x + 0 = x$ and $x \cdot 1 = x$.

F5 For every x in $\mathbb{R}$ there is an element y in $\mathbb{R}$ such that $x + y = 0$.

F6 For every $x \neq 0$ in $\mathbb{R}$ there is an element y in $\mathbb{R}$ such that $xy = 1$.

Example:

Let $\mathbb{Z}_2 = \{0, 1\}$, and define an operations $+$ and $*$ on $\mathbb{Z}_2$ by declaring that $x + y = x +_2 y$ and $x * y = x *_2 y$. So we have Cayley tables

$+$	0	1
0	0	1
1	1	0

$*$	0	1
0	0	0
1	0	1

Then $\mathbb{Z}_2$ is a field.

Consequences

(i) $a + b = a + c \implies b = c$
In particular the element 0 in **F4** is unique.

(ii) Given $a, b \in \mathbb{R}$ there is exactly one x such that $a + x = b$.
We denote this x by $b - a$. In particular $0 - a$ is written simply as $-a$ and is called the *negative* of a.

(iii) $b - a = b + (-a)$

(iv) $-(-a) = a$

(v) $a(b - c) = ab - ac$

(vi) $0 \cdot a = a \cdot 0 = 0$

(vii) $ab = ac$ and $a \neq 0 \implies b = c$
In particular the element 1 in **F4** is unique.

(viii) Given $a, b \in \mathbb{R}$ with $a \neq 0$ there is exactly one x such that $ax = b$.
This is denoted by b/a. In particular $1/a$ (or a^{-1}) is the *reciprocal* of a.

(ix) If $a \neq 0$ then $b/a = ba^{-1}$.

(x) If $a \neq 0$ then $(a^{-1})^{-1} = a$.

(xi) If $ab = 0$ then $a = 0$ or $b = 0$.

(xii) $(-a)b = -(ab)$ and $(-a)(-b) = ab$.

(xiii) $a/b + c/d = (ad + bc)/bd$ if $b \neq 0, d \neq 0$.

(xiv) $(a/b)(c/d) = ac/bd$ if $b \neq 0, d \neq 0$.

(xv) $(a/b)/(c/d) = ad/bc$ if $b \neq 0, c \neq 0, d \neq 0$.

Order Properties of $\mathbb{R}$

There is a non-empty subset P of $\mathbb{R}$ (called the set of *positive* real numbers and denoted by $\mathbb{R}^+$) such that:

O1 $x, y \in P \implies x + y,\ xy \in P$.

O2 For any $x \neq 0$ in $\mathbb{R}$ either $x \in P$ or $-x \in P$ but not both.

O3 $0 \notin P$.

We write $x < y$ iff $y - x \in P$, and $x \leq y$ iff $y - x \in P$ or $y = x$, etc.
NB It follows that $x > 0$ iff $x \in P$.

Example: $\mathbb{Z}_2$ is NOT an ordered field, although $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are.

Consequences

(i) For arbitary $x, y \in \mathbb{R}$ exactly one of the following holds
$x < y, \quad y < x, \quad x = y$ (Trichotomy)
(ii) $x < y$ and $y < z \implies x < z$ (Transitivity)
(iii) $x < y \implies x + z < y + z$
(iv) $x < y$ and $z > 0 \implies xz < yz$
(v) $x \neq 0 \implies x^2 > 0$
(vi) $1 > 0$
(vii) $x < y$ and $z < 0 \implies xz > yz$
(viii) $x < y \implies -x > -y$. In particular $x < 0 \implies -x > 0$.
(ix) $xy > 0 \implies$ both $x, y \in P$ or both x, y negative (< 0).

Remark The complex numbers cannot be ordered in a way compatible with the algebraic structure.

Absolute values

Defn If $x \in F$ (ordered field) then the *absolute value* of x is given by

$$|x| = \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x < 0. \end{cases}$$

We have $-|x| \leq x \leq |x|$ and if $a \geq 0$ then $|x| \leq a$ iff $-a \leq x \leq a$.

It is easy to see that:
(i) $|x| \geq 0$ and $|x| = 0$ iff $x = 0$.
(ii) $|x| = |-x|$.
(iii) $|x + y| \leq |x| + |y|$.

These are fundamental properties. If we write $d(x, y)$ for the distance $|x - y|$ between x and y, then
(i) $d(x, y) \geq 0$ and $d(x, y) = 0$ iff $x = y$
(ii) $d(x, y) = d(y, x)$
(iii) $d(x, y) \leq d(x, z) + d(z, y)$.
The three conditions just stated can be taken as axioms for an abstract distance function.

Some useful properties of the absolute value are

$$|x|^2 = |x^2|, \qquad |xy| = |x||y|, \qquad \big||x| - |y|\big| \leq |x - y|.$$

We can also show by induction that

$$|x_1 + x_2 + \cdots + x_n| \leq |x_1| + |x_2| + \cdots + |x_n|.$$

Integers and rationals
We have seen that $\mathbb{R}$ contains an element 1 and that $1 \in P$. So the sums $1+1, 1+1+1, \ldots$ are all distinct (otherwise some such sum would be 0 contradicting the fact that P is closed under addition).

Defn A subset S of $\mathbb{R}$ is *inductive* if
(a) $1 \in S$
(ii) $x \in S \implies x+1 \in S$ (e.g. $\mathbb{Q}, \mathbb{Q}^+$).

Defn (Positive Integers) A real number is called a positive integer if it belongs to every inductive set. We denote the set of positive integers by $\mathbb{N}$.

$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-\mathbb{N}\}$ is called the set of all integers. Quotients of integers a/b ($b \neq 0$) are called rational numbers and the set of rational numbers is denoted by $\mathbb{Q}$. Clearly $\mathbb{Z} \subset \mathbb{Q}$.

The axioms given so far define an ordered field. Since they are satisfied by both $\mathbb{R}$ and $\mathbb{Q}$ they are not sufficient to assert the existence of numbers such as $\sqrt{2}$. Before we introduce our final axiom (which achieves this goal) we need some notation.

Defn Let S be a non-empty subset of $\mathbb{R}$ and suppose there is a number $b \in \mathbb{R}$ such that $x \leq b$ for all $x \in S$. Then S is *bounded above* by b and b is an *upper bound* for S.

Remarks Every $b' > b$ is also an upper bound for S. If $b \in S$ then b is called the maximum element of S and we write $b = \max S$ (it is unique). set with no upper bound is said to be unbounded above. Similar definitions hold for *bounded below* and *lower bound*.

Examples
$\mathbb{R}^+$: unbounded above — no upper bound or maximal element.
$[0, 1]$: bounded above by 1 which is also the maximal element.
$[0, 1)$: bounded above by 1 — no maximal element.

Defn A number b is called the *least upper bound* (lub) or *supremum* (sup) of a non-empty set $s \subset \mathbb{R}$ if:
(a) b is an upper bound for S
(b) if b' is another upper bound for S the $b \leq b'$.

We write $b = \text{lub} S$. It is clearly unique. A similar definition holds for the *greatest lower bound* (glb) or *infimum* (inf). Note that lub$S$ need not belong to S. It is the "next" bigger element, e.g. $\text{lub}(0, 1) = 1$ and $\text{glb}\{1, \frac{1}{2}, \dots, \frac{1}{n}, \dots\} = 0$.

Theorem If $b = \text{lub} S$ then $x \leq b$ for all $x \in S$ and given $\epsilon > 0$ there exists $y \in S$ such that $b - \epsilon < y \leq b$.

Completeness axiom
Every non-empty set of real numbers which is bounded above has a least upper bound.

Theorem Every non-empty set S which is bounded below has a greatest lower bound.

Proof Let $-S = \{-x : x \in S\}$. Then $-S$ is non-empty and bounded above and so has a least upper bound b. But it is easily seen that $-b = \text{glb} S$.

It is not always easy to determine whether a set is bounded above or below as the following example shows.

Example Let $S = \{(1 + 1/n)^n : n = 1, 2, \dots\}$. Clearly every number in S is greater than 1 so S has a greatest lower bound. In fact glb $S = \min S = 2$. We can also show, with more difficulty, that theset is bounded above and so has a least upper bound. However the value of lub$S$ is not obvious. In fact lub$S = e$.

Archimedean Property for $\mathbb{R}$ (Consequence of completeness axiom)

Theorem The set $\mathbb{N}$ of positive integers is unbounded above.

Proof Assume false. Then since $\mathbb{N} \neq \emptyset$ it has a least upper bound b.
$\implies$ $b-1$ is not an upper bound for $\mathbb{N}$ (since $b-1 < b$).
$\implies$ there exists $n \in \mathbb{N}$ such that $b-1 < n$ i.e. $b < n+1$.
Since $n+1 \in \mathbb{N}$ this is a contradiction.

Cor 1 For every $x \in \mathbb{R}$ there exists $n \in \mathbb{N}$ such that $n > x$.
(Otherwise some x would be an upper bound for $\mathbb{N}$.)

In particular if $\epsilon > 0$ there exists $n \in \mathbb{N}$ such that $1/n < \epsilon$.

Cor 2 If $x > 0$ and if y is any real number there exists $n \in \mathbb{N}$ such that $nx > y$.
(Apply **Cor 1** with y/x for x.)

Geometrically this means that a small ruler can measure arbitrarily large distances. Archimedes realised this was a fundamental property of the number line.

Lemma If a, x, y satisfy $a \leq x \leq a + y/n$ for every integer $n \geq 1$ then $x = a$.

Proof If $x > a$ then by **Cor 2** there exists $n \in \mathbb{N}$ such that $n(x-a) > y$. But this contradicts the given inequalities. Since $x \geq a$ we must have $x = a$.

Nested Intervals Theorem
If $I_1, I_2, \ldots, I_n, \ldots$ is a set of closed intervals in $\mathbb{R}$, if $I_n \supset I_{n+1}$ for all n and if the length of I_n is less than any given $\epsilon > 0$ for all large n then there is one and only one point common to all the intervals.

Proof Let $I_n = [a_n, b_n] = \{x : a_n \leq x \leq b_n\}$. Then $a_n \leq a_{n+1} < b_{n+1} \leq b_n$ for all n since $I_{n+1} \subset I_n$. Thus $\{a_n\}$ and $\{b_n\}$ are bounded sets, e.g. $a_1 \leq a_n < b_1$ for all n.
Let $\lambda = \text{lub}\{a_n\}$, $\mu = \text{glb}\{b_n\}$. Then $\lambda \leq \mu$ and $\lambda, \mu \in \cap_n I_n$. But $\mu - \lambda < b_n - a_n$ for all n. Now $b_n - a_n$ is the length of I_n and is arbitrarily small when n is large. So $\lambda = \mu$. This point belongs to all I_n and is the only point with this property since any other point will have a distance from μ which ultimtely exceeds the length of I_n.

Remark The rational numbers $\mathbb{Q}$ satisfy the Archimedean property. So this property is not enough to characterize $\mathbb{R}$. However it can be shown that

$$\left.\begin{array}{r}\text{Archimedean property} \\ \text{+Nested intervals property}\end{array}\right\} \iff \text{Completeness property.}$$