Ordered Fields and The Real Number System

In this chapter we go over the essential, foundational, facts about the real number system.

Positive real numbers arose from geometry in Greek mathematics, as ratios of magnitudes, such as segments or planar regions or even angles. In the discussion below we focus on segments.

In Euclid's *Elements*, a segment EF is taken to exceed a segment GH, symbolically

$$EF>GH$$

if EF is congruent to a segment GK, where K is some point between E and F. An important feature of this order relation is encapsulated in the *archimedean axiom*: *given any two segments, some multiple of any one of them exceeds the other*.

Then aAa pair PQ and RS if for any positive numbers n and m, the segment nAB (which is n copies of AB laid contiguously) exceeds the segment mCD if and only if the segment nPQ exceeds the segment mRS. The ratio

$$\frac{AB}{CD}$$

is then essentially the equivalence class of all segment pairs which are in the same ratio as AB is to CD. Euclid also defines the ratio XY/ZW to be *greater* than the ratio PQ/RS :

$$\frac{XY}{ZW} > \frac{PQ}{RS}$$

if they are unequal and if whenever mZW>nXY then also mRS>nPQ.

A special case is that of *commensurate* segments: if a whole multiple of AB, say nAB, is congruent to a whole multiple of CD, say mCD, then the ratio $\frac{AB}{CD}$ is *rational*, and is denoted by

$$\frac{m}{n}.$$

It is readily checked that

$$\frac{m}{n} = \frac{p}{q}$$

if and only if

$$qm = pn.$$

Such ratios are the *rational numbers*. Other ratios are *irrational*. In either case, Euclid's considerations suggest that a ratio of segments may be understood in terms of a set of rational numbers, for example the set of all those rationals which exceed the given ratio.

The axioms of geometry, and the Euclidean construction procedures, show that ratios of segments can be added and multiplied and, when 0 and negatives are included, an algebraic structure called a *field* emerges (this is discussed at length by Hilbert [3]). The maximal such field, respecting the axioms of geometry pertaining to the order relation and congruence, constitutes the *real number system* $\mathbb{R}$.

Leaving aside the historical background, the real number system may be constructed by starting with the empty set, constructing the natural numbers, then the rationals, and then the real numbers by Dedekind's method of identifying a real number with a splitting of the rationals into two disjoint classes with members of one class exceeding those of the other.

Dedekind's method has beed generalized in a striking, and vastly more powerful way, by Conway [1], who shows how the Dedekind cut method can be applied to abstract sets leading to the construction of all real numbers as well as transcendentals and infinitesimals. Knuth's novel [4] is an unusual and entertaining presentation of this construction.

1.1 Ordered Fields

In this section we define and prove simple properties of fields, ordered fields, and absolute values. The reader wishing to move on to properties of the real numbers may skim the contents of the first few subsections, and proceed to subsection 1.1.4.

1.1.1 Fields

A *field* $\mathbb{F}$ is a set along with two binary operations

$$\text{Addition} : \mathbb{F} \times \mathbb{F} \to \mathbb{F} : (a,b) \mapsto a+b \tag{1.1}$$

and

$$\text{Multiplication} : \mathbb{F} \times \mathbb{F} \to \mathbb{F} : (a,b) \mapsto ab \tag{1.2}$$

satisfying the following axioms:

1. The associative law holds for addition

$$a+(b+c)=(a+b)+c \qquad \text{for all } a,b,c\in\mathbb{F} \tag{1.3}$$

2. There is an element $0\in\mathbb{F}$, the *zero* or *additive identity* element, for which

$$a+0=a=0+a \qquad \text{for all } a\in\mathbb{F} \tag{1.4}$$

3. Every element $a\in\mathbb{F}$ has an *additive inverse* $-a$, called the *negative* of a:

$$a+(-a)=0=(-a)+a \tag{1.5}$$

4. The commutative law holds for addition:

$$a+b=b+a \qquad \text{for all } a,b\in\mathbb{F} \tag{1.6}$$

5. The associative law holds for multiplication

6. The associative law holds for addition

$$a(bc)=(ab)c \qquad \text{for all } a,b,c\in\mathbb{F} \tag{1.7}$$

7. There is an element $1\in\mathbb{F}$, the *unit* or *multiplicative identity* element, for which

$$a1=a=1a \qquad \text{for all } a\in\mathbb{F} \tag{1.8}$$

8. Every non-zero element $a\in\mathbb{F}$ has an *multiplicative inverse* a^{-1}, called the *reciprocal* of a:

$$aa^{-1}=1=a^{-1}a \qquad \text{for all non-zero } a\in\mathbb{F} \tag{1.9}$$

9. The commutative law holds for multiplication:

$$ab=ba \qquad \text{for all } a,b\in\mathbb{F} \tag{1.10}$$

10. The *distributive law* holds:

$$a(b+c)=ab+ac, \qquad (b+c)a=ba+ca \quad \text{for all } a,b,c\in\mathbb{F} \tag{1.11}$$

11. The element 1 is not equal to the element 0:

$$1\neq 0$$

We have not attempted to provide a minimal axiom set, and some of the axioms may be deduced from others. For instance, the commutativity of addition can be deduced from the other axioms.

Because of the associative laws, we will just write

$$a+b+c$$

instead of $a+(b+c)$, and

$$abc$$

instead of abc.

Let us note a few simple consequences:

Theorem 1 *If $x \in \mathbb{F}$ is such that*

$$a+x=a \quad \textit{for some } a \in \mathbb{F}$$

and $y \in \mathbb{F}$ is such that

$$by=b \quad \textit{for some non-zero } b \in \mathbb{F}$$

then

$$x=0 \qquad \textit{and} \qquad y=1.$$

In particular, the additive identity and the multiplicative identity are unique. Moreover,

$$-0=0 \qquad \textit{and} \qquad 1^{-1}=1$$

Proof. Adding $-a$ to

$$a+x=a$$

shows that x is 0. Multiplying

$$by=b$$

by b^{-1} shows that y is 1. The other claims follow from

$$0+0=0 \qquad \text{and} \qquad 1\cdot 1=1.\ \boxed{\text{QED}}$$

Theorem 2 *If $a, b \in \mathbb{F}$, and $b \neq 0$, then*

$$-(-a) = a, \qquad \textit{and} \qquad (b^{-1})^{-1} = b.$$

Moreover,

$$(-a)b = -ab, \qquad \textit{and} \qquad (-a)(-b) = ab.$$

The multiplicative inverse a^{-1} is best written as the reciprocal:

$$\frac{1}{b} = b^{-1},$$

and the product ab^{-1} as

$$\frac{a}{b} = ab^{-1}$$

There are many other easy consequences of the axioms which we will use without comment.

We denote the set of *natural numbers* by $\mathbb{P}$:

$$\mathbb{P} = \{1, 2, 3, ...\}, \tag{1.12}$$

and the set of *integers* by

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, ...\}, \tag{1.13}$$

We can multiply any element $a \in \mathbb{F}$ by an integer as follows. First define

$$1a = a,$$

where now 1 is the number one in $\mathbb{Z}$. Next,

$$2a \stackrel{\text{def}}{=} a + a,$$

and, inductively,

$$(n+1)a \stackrel{\text{def}}{=} na + a \tag{1.14}$$

for all $a \in \mathbb{F}$ and all $n \in \mathbb{P}$. Next define negative multiples by

$$(-n)a = -(na) \tag{1.15}$$

for all $n \in \mathbb{P}$ and all $a \in \mathbb{F}$. Finally,

$$0a = a \tag{1.16}$$

where 0 is the integer 0. The following facts can be readily verified:

$$x(ya) = (xy)a \quad \text{for all } x,y \in \mathbb{Z} \text{ and all } a \in \mathbb{F} \tag{1.17}$$
$$x(a+b) = xa+xb \quad \text{for all } x \in \mathbb{Z} \text{ and all } a,b \in \mathbb{F} \tag{1.18}$$
$$(x+y)a = xa+ya \quad \text{for all } x,y \in \mathbb{Z} \text{ and all } a \in \mathbb{F} \tag{1.19}$$

There is a multiplicative analog of this given by powers of elements. If m is a positive integer and $a \in \mathbb{F}$ we define

$$a^1 = a$$

and

$$a^{m+1} = a^m a.$$

We also define

$$a^0 = 1 \qquad \text{for non-zero } a \in \mathbb{F}$$

and, for any positive integer m and non-zero $a \in \mathbb{F}$,

$$a^{-m} = (a^{-1})^n = \frac{1}{a^m}$$

We will use without comment simple facts such as

$$(a^m)^n = a^{mn},$$

valid for suitable $a \in \mathbb{F}$ and $m,n \in \mathbb{Z}$.

The simplest example of a field is the two-element field

$$\mathbb{Z}_2 = \{0,1\},$$

with addition and multiplication defined modulo 2; for example,

$$1+1 = 0 \qquad \text{in } \mathbb{Z}_2$$

We will, however, be concerned with fields which permit a consistent ordering of their elements.

1.1.2 Order Relations

An *order relation* on a set S is a set O of ordered pairs (x,y) of elements of S satisfying the conditions O1 and O2 below. It is convenient to adopt the convention that

$$x < y \text{ means } (x,y) \in O$$

We also write

$$y > x$$

to mean $x < y$. The axioms of order are:

O1. For any $x, y \in \mathbb{F}$ exactly *one* of the following hold:

$$x = y, \quad \text{or} \quad x < y, \qquad \text{or} \quad y < x.$$

O2. If $x < y$ and $y < z$ then $x < z$.

It is also convenient to use the notation:

$$x \leq y \text{ means } x = y \text{ or } x < y$$

and, similarly,

$$x \geq y \text{ means } x = y \text{ or } x > y$$

If T is a subset of an ordered set S then an element $u \in S$ is said to be an *upper bound* of T if

$$t \leq u \quad \text{for all } t \in T \tag{1.20}$$

If there is a least such upper bound then that element is called the *supremum* of T:

$$\sup T = \text{the least upper bound of } T \tag{1.21}$$

We define similarly *lower bounds* and *infimums*:

$$\text{if } l \leq t \text{ for every } t \in T \text{ then } l \text{ is called a lower bound of } T \tag{1.22}$$

and

$$\inf T = \text{ the greatest lower bound of } T \tag{1.23}$$

Of course, the sup or the inf might not exist.

1.1.3 Ordered Fields

An *ordered field* is a field $\mathbb{F}$ with an order relation in which, in addition to the field and order axioms stated above, the following hold:

OF1. If $x, y, z \in \mathbb{F}$ and $x < y$ then $x + z < y + z$:

$$x < y \text{ implies } x + z < y + z \text{ for all } x, y, z \in \mathbb{F} \tag{1.24}$$

OF2. If $x, y, z \in \mathbb{F}$ and $x < y$, and if also $z > 0$, then $xz < yz$:

$$x < y \text{ and } z > 0 \text{ imply } xz < yz \text{ for all } x, y, z \in \mathbb{F}. \tag{1.25}$$

If $x > 0$ we say that x is *positive*. If $x < 0$ we say that x is *negative*.
We have the following simple observations for an ordered field:

Theorem 3 *Let $\mathbb{F}$ be an ordered field. Then*

(i) $x > 0$ *if and only if* $-x < 0$

(ii) For any non-zero $x \in \mathbb{F}$ *we have* $x^2 > 0$

(iii) $1 > 0$

(iv) For any $r \in \mathbb{Z}$ *the element* $r1 \in \mathbb{F}$ *is* > 0 *if* r *is a positive integer and is* < 0 *if* r *is a negative integer*

(v) $x > y$ *holds if and only if* $x - y > 0$

(vi) If $x \in \mathbb{F}$ *and* $x > 0$ *then* $1/x > 0$

(vii) The product of two positive elements is positive

(viii) The product of a positive and negative is negative

(ix) The product of two negative elements is positive

(x) If $x > y$ *and* $z < 0$ *then* $xz < yz$.

(xi) If $x > y$ *then* $-x < -y$

(xii) If $x > y > 0$ *then* $1/x < 1/y$

Proof. We prove some of the results.
(i) Suppose $x > 0$. Then we have

$$x + (-x) > 0 + (-x),$$

and so

$$0 > -x.$$

Conversely, if $-x < 0$ then adding x to both sides shows that $x > 0$.

(ii) If $x > 0$ then, by OF2, we have

$$x^2 = xx > x0 = 0.$$

On the other hand, if $x < 0$ then we know that $-x > 0$ and so

$$x^2 = (-x)(-x) > (-x)0 = 0.$$

(iii) Since 1 is 1^2, it follows that $1 > 0$.

(vi) Suppose $x > 0$. Since $x(1/x) = 1$, and $1 \neq 0$, it follows that $1/x$ cannot be zero. If $1/x < 0$ then, however, $x(1/x)$ would have to be < 0, but we know that $1 > 0$. Thus, $1/x > 0$.

(xi) If $x > y$ then, adding $-x - y$ shows that $-y < -x$.

(xii) If $x > y > 0$ then $xy > 0$ and hence $1/(xy) > 0$. Multiplying $x > y$ by the positive element $1/(xy)$ gives $1/y > 1/x$. $\boxed{\text{QED}}$

Observe that if $x > 0$ then

$$2x = x + x > x + 0 = x,$$

and

$$3x = 2x + x > 2x + 0 = 2x,$$

and, proceeding inductively, we have

$$0 < x < 2x < 3x < \cdots < nx < (n+1)x < \cdots \qquad \text{for all } n \in \mathbb{P} \text{ and } x > 0 \text{ in } \mathbb{F} \tag{1.26}$$

In particular, inside the ordered field $\mathbb{F}$ we have a copy of the natural numbers $1, 2, 3, \ldots$ on identifying $n \in \mathbb{P}$ with $n1_{\mathbb{F}}$, where $1_{\mathbb{F}}$ is the unit element in $\mathbb{F}$. This then leads to a copy of the integers inside $\mathbb{F}$, and we can assume that

$$\mathbb{Z} \subset \mathbb{F} \tag{1.27}$$

Going further, if $m, n \in \mathbb{Z}$, and $n \neq 0$, we have then the ratio

$$\frac{m}{n} \in \mathbb{F}.$$

The set of all such ratios m/n is the set of *rationals*

$$\mathbb{Q} \subset \mathbb{F} \tag{1.28}$$

and is an ordered subfield of the ordered field $\mathbb{F}$.

1.1.4 The absolute value function

The *absolute value* $|\cdot|$ function in an ordered field $\mathbb{F}$ is defined by

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x \leq 0 \end{cases} \tag{1.29}$$

For instance,

$$|1| = 1, \quad \text{and} \quad |-1| = 1.$$

The definition of $|x|$ shows directly that

$$|-x| = |x| \geq 0 \qquad \text{for all } x \in \mathbb{F} \tag{1.30}$$

It is also useful to observe that

$$|x| \text{ is the larger of } x \text{ and } -x \tag{1.31}$$

We think of

$$|a-b|$$

as measuring the *difference* between a and b.

We have then

Theorem 4 *For any $a,b \in \mathbb{F}$ we have:*

(i) the **triangle inequality**

$$|a+b| \leq |a| + |b| \tag{1.32}$$

Equality holds if and only if a and b are both ≥ 0 or both ≤ 0.

(ii) the absolute values differ by at most the difference in a and b:

$$\big||a| - |b|\big| \leq |a-b| \tag{1.33}$$

(iii) $|ab| = |a||b|$.

Proof. Recall that $|x|$ is the larger of x and $-x$. Therefore, $|a|+|b|$ is greater or equal to $\pm a+(\pm b)$; in particular, it is greater or equal to $a+b$ and $(-a)+(-b)$. Consequently, $|a|+|b|$ is greater or equal to $a+b$ and $-(a+b)$, and so

$$|a|+|b| \geq |a+b|.$$

Equality holds if and only if $|a|=a$ and $|b|=b$ or $|a|=-a$ and $|b|=-b$. Thus, equality holds if and only if a and b are either both ≥ 0 or both ≤ 0.

Next, using the triangle inequality we have

$$|a-b|+|b| \geq |a+b-b| = |a|,$$

and so

$$|a-b| \geq |a|-|b|.$$

Interchanging a and b yields:

$$|b-a| \geq |b|-|a|.$$

Observe that

$$|b-a| = |a-b|.$$

Thus,

$$|a-b| \text{ is } \geq \text{ to both } |a|-|b| \text{ and } -(|a|-|b|).$$

Since the larger of the latter is $\big||a|-|b|\big|$, we have proved (1.33).

We know that $|x|$ is x or $-x$, whichever is ≥ 0. Consequently, the product $|a||b|$ is one of the elements

$$ab, (-a)b, a(-b), (-a)(-b),$$

i.e. one of the elements ab and $-ab$. Thus, $|a||b|$ is ab or $-ab$, whichever is ≥ 0, and so it is $|ab|$. QED

1.1.5 The Archimedean Property

An ordered field $\mathbb{F}$ is said to have the *archimedean* property if for any $x, y \in \mathbb{F}$, with $x > 0$, there exists a multiple of x which exceeds y:

$$nx > y \text{ for some } n \in \{1, 2, 3, \ldots\} \tag{1.34}$$

The field $\mathbb{Q}$ of rationals is clearly archimedean:

Theorem 5 *The ordered field $\mathbb{Q}$ of rationals is acrhimedean.*

Proof. Let $x, y \in \mathbb{Q}$, with $x > 0$. If $y \geq 0$ then we have $1x > y$ and we are done. Now suppose $x, y > 0$. Then

$$x = \frac{p}{q} \quad y = \frac{r}{s},$$

where $p, q, r, s \in \mathbb{P}$. Take

$$n = qr + 1.$$

Then

$$nx = qr(p/q) + p/q > pr \geq \frac{r}{s} = y,$$

and we are done. QED

In an archimedean ordered field there are no infinities, and there are also no infinitesimals:

Theorem 6 *If $\mathbb{F}$ is an archimedean field then for any $w > 0$ in $\mathbb{F}$ there is an $n \in \mathbb{P}$ such that*

$$\frac{1}{n}w < x.$$

Proof. Simply choose n for which nx is $> w$. QED

1.2 The Real Number System $\mathbb{R}$

We shall work with the real number system in an axiomatic way. We will assume that it is an ordered field in which the completeness axiom of completeness holds.

Needless to say, it is essential to actually *construct* such a system so as to be sure that there is no hidden contradiction between the axioms, but we shall not describe a construction in these notes.

1.2.1 Hilbert Maximality and the Completeness Property

As we have mentioned before, the structure of Euclidean geometry, as formalized through the axioms of Hilbert, produces an archimedean ordered field. To complete the story, one can add to these axioms the further requirement that this field is maximal in the sense that it cannot be embedded inside any larger archimedean ordered field. It turns out then that any such ordered field is isomorphic to any other, and thus there is essentially one such ordered field. This ordered field is the real number system $\mathbb{R}$.

A crucial fact about $\mathbb{R}$ is the *completeness* property:

> *If L and U are non-empty subsets of $\mathbb{R}$ such that every element of L is $\leq$ every element of U, then there is a real number m which lies between L and U:*
>
> $$l \leq m \leq u \text{ for all } l \in L \text{ and all } u \in U. \tag{1.35}$$

This property is also often expressed as:

> *If $\mathbb{R}$ is partitioned into two disjoint subsets L and U whose union is $\mathbb{R}$, and if every element of L is $\leq$ every element of U then there is a unique element $x \in \mathbb{R}$ which lies between L and U:*
>
> $$l \leq x \leq u \text{ for all } l \in L \text{ and all } u \in U. \tag{1.36}$$

It is useful to view the real numbers geometrically. Consider a line, with two special points O and I marked on it. For any point P on the line on the same side of O as P we think of the ratio OP/OI as a positive real number. Points on the other side from I correspond to negative real numbers, and the point O itself should be thought of as 0. The completebess property says that there are no 'gaps' in the line.

The completeness property can be formulated equivalently as:

Every non-empty subset of $\mathbb{R}$ which has an upper bound has a least upper bound. (1.37)

The completeness property implies the archimedean peoperty:

Theorem 7 *If in an ordered field the property (1.37) holds then the archimedean property also holds.*

A proof of this is outlined in an exercise below.

The modern understanding and point of view on completeness grew out of the work of Richard Dedekind [2].

1.2.2 Completeness of $\mathbb{R}$ and measurement

Even in Euclid's geometry, a real number was, implicitly, understood in terms of all rationals which exceeded it and all rationals below it. However, the traditional axioms of Euclidean geometry, with requirements on intersections of lines and circles, can work with a field which is larger than the rationals but smaller than $\mathbb{R}$, and completeness is not essential.

The simplest measurement problem is to devise a measure of sets of points in the plane which are made up of a finite collection of segments constructed by Euclidean geometry. Two such sets should have the same measure if they can be decomposed into a finite collection of congruent segments. For this we would not need the full complete system $\mathbb{R}$ of real numbers. Moving up a dimension, with the task of measuring areas of polygonal regions constructed by Euclidean geometry, one could still get away with a less-than-complete system of numbers. However, it was shown by Max Dehn in 1900, in resolving Hilbert's Third Problem, that there are polyedra in three dimensions which have equal volumes (as defined by requirements of 'upper' and 'lower' approximations) which cannot be decomposed into congruent pieces. This, along with, of course, the utility of measuring areas of curved regions even in two dimensions, makes it absolutely essential to work with a notion of measure that goes beyond simply decomposing into geometrically congruent figures. For a truly useful theory of measure, the completeness of the number system is essential.

Capturing a real number between upper approximations and lower approximations proves to be very useful. Archimedes and others computed areas of curved regions by such upper and lower approximations. In modern calculus, this method lives on in the Riemann integral, as we shall see later.

Problem Set 1

1. Prove that in any ordered field, between any two distinct elements there is at least one other element.

2. Prove that in any ordered field, between any two distinct element lie infinitely many elements.