1 Real and Complex Numbers

1.1 Desired Properties

Let us begin by asking what one would like to have in the number system one works with? As a child grows up, he/she first learns about the collection $\mathtt{N}$ of *counting numbers*, which mathematicians like to call the *natural numbers*, then proceeds to the all important *zero* and *negative numbers*, and after that to *fractions*, often called the *rational numbers*. What one has at that point is a very elegant system of numbers with all the desired *arithmetical operations* and the important notion of *positivity*. This last property allows one to partition the rationals into *positive numbers*, *negative numbers* and zero, and thereby define an *ordering* on the set $\mathtt{Q}$ of all rational numbers, namely the stipulation that $a \leq b$ iff $b-a$ is either positive or 0. One defines a number b to be an *upper bound* (resp. a *lower bound*) for a set X of rationals iff every x in X satisfies $x \leq b$ (resp. $b \leq x$). The set X is said to be *bounded above*, resp. *bounded below*, if it admits an upper bound, resp. lower bound; it is *bounded* if both bounds exist. Of course any finite set of rationals is bounded, but infinite sets like $\{\frac{1}{n} \,|\, n \in \mathtt{N}\}$ are bounded too.

One could stay in this rational paradise for a long time and find many treasures to unearth, but one runs into *two related problems*. The first problem is that various numbers one encounters in *real life*, for example the hypotenuse ($= \sqrt{2}$) of any right triangle with unit sides and the circumference ($= 2\pi$) of the unit circle, are not rational numbers, though historically it took a while for people to *prove* their *irrationality*. The second problem is that given a bounded set of rational numbers there is usually no rational number b which is a *least upper bound* (*lub*), also called a *supremum*, i.e., having the property that if b_1 is any upper bound for X, then $b \leq b_1$. A natural example is furnished by the (bounded) set

$$X_0 \,=\, \{\sum_{m=1}^{n} \frac{1}{m!} \,|\, n \geq 1\}. \tag{1.1.1}$$

Similarly, a general X has no *greatest lower bound glb*, often called an *infimum*. (But X_0 does have an infimum, namely 1.)

Note that the least upper bound will be unique if it exists. Indeed, if b, b' are suprema of a bounded set X, then $b \leq b'$ and $b' \leq b$, yielding $b = b'$.

One is thus led to enlarge $\mathtt{Q}$ to get a bigger number system, to be called the set $\mathtt{R}$ of *real numbers*, which solves the second problem above while still preserving the basic properties of $\mathtt{Q}$ including positivity. We want the following properties to hold:

[$\mathcal{R}1$] $\mathtt{R}$ admits the four basic arithmetical operations;

[$\mathcal{R}2$] There is a subset P of (*positive*) real numbers, closed under addition and multiplication, such that $\mathtt{R}$ is the disjoint union of P, 0 and $-P$; and

[$\mathcal{R}3$] Every subset X which is bounded above admits a least upper bound.

In addition one also wants to make sure that this larger system is not too big; it should *hug* the rational numbers ever so tightly. To phrase it mathematically, one wants the following to hold as well:

[$\mathcal{R}4$] Given any two distinct numbers x, y in $\mathtt{R}$, there is a rational number a such that $x < a < y$.

It turns out that there is a unique number system satisfying properties $\mathcal{R}1$ through $\mathcal{R}4$, which we call $\mathtt{R}$. These properties are extremely important and will be repeatedly used, implicitly or explicitly, in Calculus and in various other mathematical disciplines.

Often one thinks of $\mathtt{R}$ as a collection of decimal expansions, with a natural equivalence (like $1.9999\cdots = 2$), and the rationals are characterized as the ones with eventually repeating blocks of digits; for example, $\frac{22}{7}$ is represented by $3.142857142857142857142857\ldots$. (A justification for this way of thinking of $\mathtt{R}$ will come later, after we learn about Cauchy sequences and completion in chapter 2.) From this point of view, one sees quickly that there is nothing terribly real abut the real numbers, as no one, and no computer, can remember the *entire* decimal expansion of an irrational number, only a suitably truncated rational approximation, like $\frac{22}{7}$, or better, $3.14159265358979323846 = \frac{314159265358979323846}{100000000000000000000}$, for π. One does encounter irrational numbers in nature, as mentioned above, but usually in *Geometry* or *Differential equations*.

In the case of the set X_0 of (1.1.1), the unique (irrational) supremum is the ubiquitous number e, whose decimal expansion is $2.718281828459045235306\ldots$.

It should be remarked that fortunately, the first problem encountered while working only with Q gets essentially solved in R: The irrational numbers $\sqrt{2}$ and π, and a whole slew of others like them, belong to, i,e., represented by numbers in, the system R. Qualitatively, however, there is a huge difference between $\sqrt{2}$ and π. The former is what one calls an *algebraic number*, i,e., one satisfying a *polynomial equation* with coefficients in Q. A number which is *not* a root of any such polynomial is called a *transcendental number*; π is one such and e is another. For a long time people could not prove the existence of transcendental numbers, or rather they could not prove that the numbers like e and π, which they suspected to be transcendental, were indeed so. We do not know to this day the status of the numbers $e + \pi$ and $e\pi$, which is a terrific open problem. One could also show the existence of transcendental numbers by showing that algebraic numbers are *countable* while R is not.

Yes, R is great to work with for a lot of purposes. But it is not paradise either. This is because a lot of algebraic numbers are not to be found in R. To elaborate, the irrational number $\sqrt{2}$ is a root of the polynomial $x^2 - 2$, i.e., a solution of the equation $x^2 = 2$. Why restrict to this polynomial? How about $x^3 - 2$ or $x^2 + 1$? It turns out that $x^3 - 2$, and indeed any polynomial of odd degree, has a real root (as we will see later in the course), though R does not contain all the roots; so things are not too bad here. On the other hand, one can prove that R cannot contain any root of $x^2 + 1$; the situation is the same for $x^2 + a$ for any positive number a. Historically people were so stumped by this difficulty that they called the square roots of negative numbers *imaginary numbers*, which is unfortunate. Just like the real numbers aren't so real, imaginary numbers aren't so imaginary. We will however bow to tradition and stick to these terms.

In any case, one is led to ask if one can enlarge R further to develop a number system solving this problem. The solution which pops out is the system C of *complex numbers*, which is unique in a natural sense. One has the following properties:

[$\mathcal{C}1$] The four basic arithmetical operations extend to C; and

[$\mathcal{C}2$] Every polynomial with coefficients in C has a root in C.

The property $\mathcal{C}2$ is often called the *Fundamental Theorem of Algebra*. For this reason one wants to work with C instead of R. For example, this

property allows one to be able to find eigenvalues and eigenvectors of real symmetric matrices, and this is important in both *Linear Algebra* (Ma1b material) and *Differential Equations* (Ma2b material).

Note however that the ordering property of `Q` and `R` (coming from their positive elements) seems to have evaporated in the context of `C`. This is indeed the case, and this goes to show that everything has its drawbacks, and one has to carefully choose the system one works with, depending on the problem to be solved. In any case, much of Ma1a will deal with `R`, but sometimes also with `C`.

1.2 Natural Numbers, Well Ordering, and Induction

We will begin by admitting that everyone knows about the set `N` of natural numbers, namely the collection $\{1, 2, 3, \ldots, n, n+1, \ldots\}$. We are appealing here to one's intuition and not giving a mathematical definition, which is subtle. Interested students can consult Chapter I of the book *Foundations of Analysis* by E. Landau.

Given any two numbers a, b in `N`, one can add them as well as multiply them, and the results are denoted respectively by $a + b$ and ab (denoted at times by $a.b$ or $a \times b$). One has

$$(F1) \qquad a + b = b + a$$

$$(F2) \qquad (a + b) + c = a + (b + c)$$

$$(F3) \qquad ab = ba$$

$$(F4) \qquad (ab)c = a(bc)$$

and

$$(F5) \qquad (a + b)c = ab + ac.$$

It is customary to call the property (F1) (resp. (F3)) *commutativity* of addition (resp. multiplication), and the property (F2) (resp. (F4)) *associativity* for addition (resp. multiplication). Property (F5) is called *distributivity*.

The reason for enumerating these as (Fn), for $n \leq 5$, is that they will later become parts of the axioms for a *field*.

The fundamental property underlying the basic structure of $\mathtt{N}$ is the following

Well Ordering (WO): *Every non-empty subset S of $\mathtt{N}$ contains a smallest element m, i.e., $m \leq x$ for every x in S.*

When $S = \mathtt{N}$, m is the *unit element* 1, satisfying (for all x)

$$(F6) \qquad 1 \cdot x \;=\; x \cdot 1 \;= x.$$

A very useful thing to employ in all of Mathematics is induction, which we will now state precisely.

Principle of Mathematical Induction (PMI): *A statement P about $\mathtt{N}$ is true if*

(i) P holds for $n = 1$; and

(ii) If $n > 1$ and if P holds for all $m < n$, then P holds for n.

Lemma *WO $\implies$ PMI.*

Proof. Suppose (i), (ii) hold for some property P.
To show: P is true for all non-negative integers.
Prove by contradiction. Suppose P is false. Let S be the subset of $\mathtt{N}$ for which P is false. Since P is assumed to be false, S is non-empty. By WO, there exists a **smallest** element n of S, which is > 1 as P holds for 1. Since n is the smallest for which P is false, P must hold for *all* $m < n$. Hence by (ii), P holds for n as well. **Contradiction!** So P holds.
□

Remark: In fact, PMI and WO are equivalent. Interested students are invited to try and show the reverse implication PMI $\Rightarrow$ WO.

Example: Let us prove by induction the formula

$$1^3 + 2^3 + \ldots + n^3 \;=\; \frac{n^2(n+1)^2}{4}.$$

It evidently holds for $n = 1$, and so let us assume that n is > 1, and assume by induction that the formula holds for all $m < n$. In particular it holds for $n - 1$, and we get

$$1^3 + 2^3 + \ldots + (n-1)^3 + n^3 \;=\; \frac{(n-1)^2 n^2}{4} + n^3 \;=\; \frac{n^2((n-1)^2 + 4n)}{4},$$

which yields the asserted formula as $(n-1)^2 + 4n = (n+1)^2$.

1.3 Integers

In order to get all the integers, one needs to add to $\mathtt{N}$ the number 0, sometimes called the *additive identity*, satisfying

$$(F7) \qquad a + 0 \;=\; 0 + a \;=\; a,$$

and the *negative numbers* $-a$ $(= (-a))$, a *unique* one for each a in $\mathtt{N}$, such that

$$(F8) \qquad a + (-a) \;=\; (-a) + a \;=\; 0.$$

It is customary to call $-a$ the *negative*, or the *additive inverse*, of a. One defines *subtraction* by setting

$$a - b \;=\; a + (-b).$$

One also sets

$$-0 \;=\; 0 \quad \text{and} \quad 0 + 0 \;=\; 0.$$

One can deduce various other identities from these, for example:

$$-(-a) \;=\; a, \quad \text{and} \quad a - b \;=\; -b + a \;=\; -(b - a).$$

The discovery of *zero* was a major achievement in human history, and it happened long after the appearance of natural numbers. Put

$$-\mathtt{N} \;=\; \{-n \,|\, n \in \mathtt{N}\}.$$

By the *set of integers* one means

$$\mathtt{Z} \;=\; -\mathtt{N} \cup \{0\} \cup \mathtt{N} \;=\; \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

One calls $\mathtt{N}$, resp. $-\mathtt{N}$, the *set of positive integers*, resp. the *set of negative integers*.

Note the following assertions for elements of $\mathtt{Z}$:

($Ord1$) Every a is either positive or negative or zero;

($Ord2$) If a, b are positive, then $a + b$ and ab are also positive.

This defines an *ordering* on $\mathtt{Z}$ given by

(Ord) $$a > b \Leftrightarrow a - b \in \mathtt{N}.$$

We will also put

$$a \geq b \Leftrightarrow a = b \quad \text{or} \quad a > b,$$

and

$$a \leq b \Leftrightarrow b \geq a \quad \text{and} \quad a < b \Leftrightarrow b > a.$$

We will come back to this important notion of ordering later.

Of course one can add, resp. multiply, any *finite* number of elements, say $a_1, a_2, \ldots a_n$ of $\mathtt{Z}$, and we will use the symbolic notation

$$\sum_{j=1}^{n} a_j =, a_1 + a_2 + \ldots + a_n$$

resp.

$$\prod_{j=1}^{n} a_j = a_1 a_2 \ldots a_n.$$

We will use the convention that an *empty sum* is zero, while an *empty product* is 1.

Finally, we should note that $\mathtt{Z}$ *is countable*. Indeed, consider the function

$$f : \mathtt{Z} \to \mathtt{N},$$

defined by setting $f(0) = 1$ and for n positive,

$$f(n) = 2n \quad \text{and} \quad f(-n) = 2n + 1.$$

It is easy to check that this function is one-to-one and onto, as desired.

1.4 Rational Numbers

Given any a in $\mathtt{Z}$, we know that it has an additive inverse, namely $-a$, satisfying $(F8)$. But how about a *multiplicative inverse*? For this we need to find a number b such that

$$ab = 1.$$

But a little rumination will assure one that the only possibility is $a = b = \pm 1$. This is not good as one would like to have a multiplicative inverse for every non-zero a in $\mathtt{Z}$.

This problem is solved by the introduction of *rational numbers*. It is achieved as follows.

By an *ordered pair* of integers we will mean a pair (m, n), $m, n \in \mathtt{Z}$, where the order matters, i.e., (m, n) is considered to be different from (n, m). One denotes the collection of all ordered pairs of integers by $\mathtt{Z}^2$ (or $\mathtt{Z} \times \mathtt{Z}$). Set

$$Y = \{(m, n) \,|\, n \neq 0\}.$$

Introduce a multiplication in $\mathtt{Z}^2$ by

$$(m, n)(m', n') = (mm', nn').$$

If nn' is zero, then n or n' must be zero, and this implies that this multiplication preserves Y, i.e., the product of any two elements of Y is in Y.

Define a relation $\sim$ on Y by the requirement

$$(m, n) \sim (m', n') \Leftrightarrow mn' = m'n.$$

It is left as an easy exercise to check that that this gives an *equivalence relation* on Y.

Put

$$\mathtt{Q} = Y/\sim .$$

This is the set of *rational numbers*. As discussed in section 0.4, the elements of $\mathtt{Q}$, called the *rational numbers* (or *fractions*) are *equivalence classes* in Y. The equivalence class of any ordered pair (m, n) of integers with $n \neq 0$ is denoted $\frac{m}{n}$. By definition,

$$\frac{a}{b} = \frac{ad}{bd} \quad \forall d \in \mathtt{Z}, d \neq 0.$$

It is customary to call this the *cancellation property* of fractions. For instance,

$$\frac{2}{3} = \frac{14}{21} = \frac{100}{150} = \frac{1382}{2073}.$$

Since -1 is non-zero, we have in particular,

$$\frac{-m}{n} = \frac{m}{-n},$$

which we will simply denote by $-\frac{m}{n}$ and call it the *negative* of $\frac{m}{n}$.

Addition of rational numbers is defined by

$$\frac{m}{n} + \frac{m'}{n'} = \frac{mn' + +m'n}{nn'}.$$

The multiplication on Y gives rise to a (commutative) multiplication in $\mathtt{Q}$. Explicitly,

$$\frac{m}{n}\frac{m'}{n'} = \frac{mn}{m'n'}.$$

Given a rational number $\frac{m}{n}$, it is customary to represent it by its *reduced fraction*, i.e., write it as $\frac{m'}{n'}$ with m', n' being relatively prime, with m', n' (necessarily) satisfying $m = dm'$ and $n = dn'$, where d denotes the *gcd* of m, n.

Note that we can view $\mathtt{Z}$ as a subset of $\mathtt{Q}$ by the identification

$$m = \frac{m}{1} \quad \forall m \in \mathtt{Z},$$

compatible with multiplication, addition and subtraction. We will not make any distinction (at all) between m and $\frac{m}{1}$.

Now we are ready to find multiplicative inverses. Suppose $a = \frac{m}{n}$ is a non-zero rational number. Then m is not zero either, and so we can consider the rational number $b = \frac{n}{m}$. Then we have

$$ab = \frac{m}{n}\frac{n}{m} = \frac{mn}{nm} = \frac{mn}{mn} = 1.$$

The last (cancellation) step is justified because mn is non-zero. Since the multiplication in $\mathtt{Q}$ is commutative, ba is also 1, and so b is the *multiplicative inverse* of a.

In particular, since $\mathtt{Z}$ is a subset of $\mathtt{Q}$, every integer m has a multiplicative inverse, namely $\frac{1}{m}$.

To repeat, we have in $\mathtt{Q}$:

$$(F9) \qquad \forall a \neq 0,\ \exists b \quad \text{s.t.} \quad ab = ba = 1.$$

We will say that a rational number a is *positive* if it is given by a fraction $\frac{m}{n}$ with m, n of the same sign. A rational number whose negative is positive will be said to be *negative*. This introduces an ordering in $\mathtt{Q}$ as in the case of $\mathtt{Z}$.

It will be left as an exercise to show that the properties $(F1) - (F8)$ as well as $(Ord1)$ and $(Ord2)$ hold in $\mathtt{Q}$. We have already seen that $(F9)$ holds in $\mathtt{Q}$.

It is useful to note the following

Lemma *Given rational numbers a, b with $a < b$, we can find another rational number c with $a < c < b$.*

Proof. Put $x = b - a$, which is a positive rational number. It suffices to show that there is a positive rational number y less than x, for then we can take c to be $a + y$. Write $x = \frac{m}{n}$, for some positive integers m, n. Then $y = \frac{m}{n+1}$ does the job. In fact, $\frac{m}{n+k}$ works for *every* $k \geq 1$. Done. □

Note that the proof shows that there are in fact an infinite number of rational numbers between a and b.

We conclude this section by noting that it can be shown that $\mathtt{Q}$ is a *countable* set. Try to construct a one-to-one correspondence between $\mathtt{Q}$ and $\mathtt{N}$.

1.5 Ordered Fields

Any set K admitting addition and multiplication, equipped with distinguished elements called 0 and 1, for which the properties (*axioms*) $(F1)$ through $(F9)$ hold, is called a *field*.

As we have seen above, $\mathtt{Q}$ is a field. But there are others, and here is a very simple one. Put

$$\mathtt{F}_2 = \{0, 1\},$$

and define addition by the rule

$$0+0=0, \quad 0+1=1+0=1 \quad \text{and} \quad 1+1=0,$$

and multiplication by the rule

$$0\times 0=0, \quad 0\times 1=1\times 0=0 \quad \text{and} \quad 1\times 1=1.$$

It is clear that the axioms $(F1)-(F9)$ are satisfied making $\mathtt{F}_2$ a field with only two elements. Check that there can be no field with just 1 element.

In order to do Calculus, we must restrict the fields we consider. Say that a field K is an *ordered field* if the properties $(Ord1)$ and $(Ord2)$ also hold in K relative to an ordering $\leq$. We know that $\mathtt{Q}$ is an ordered field. Is there any other? It is immediate that $\mathtt{F}_2$ is *not* an ordered field, because 1 is its own negative there.

As remarked in section 1.0, $\mathtt{Q}$ suffers in general from a lack of *least upper bounds* for its bounded subsets. For this reason we want to enlarge it. To this end, we are motivated to define a *complete ordered field* to be an ordered field K in which the following holds:

$(Cord)$ Every bounded subset X admits a least upper bound, i.e., there exists a b such that if for some b', $x\leq b'\,\forall x\in X$, then $b\leq b'$.

The first question is is to know if there is *any* complete ordered field. An affirmative answer will be given in the next section.

1.6 Real Numbers

The object of this section is to give a construction of all *real numbers* and show that they form a complete ordered field $\mathtt{R}$ containing $\mathtt{Q}$. They will satisfy the properties $(\mathcal{R}1)$ through $(\mathcal{R}4)$ of section 1.0. To some the construction might appear to be too abstract, at least on a first reading. One does not have to master the proof, but it is important to feel comfortable enough with the basic properties of real numbers and learn to use them at moment's notice. We will also discuss a different construction of $\mathtt{R}$ in the next chapter, after introducing Cauchy sequences and completion from that point of view; some will find that (*analytic*) approach more understandable, while others will like

the present (*algebraic*) approach due to a nineteenth century mathematician called R. Dedekind.

The basic idea is this. Geometrically, the rational numbers represent a special collection of points on a line L with 0 in the middle and the integers being plotted in the usual way. Intuitively, one would like to have the points on the line be in one-to-one correspondence with the real numbers. But how to achieve this when all one could define precisely are the rational numbers. Dedekind's clever observation was that giving a rational number a is the same as giving the set τ_a of all the rational numbers to the left of, i.e., strictly less than, a on L. Moreover, $a \leq b$ iff $\tau_a \leq \tau_b$, and τ_{a+b} is given by the set, to be called $\tau_a + \tau_b$, consisting of rational numbers c which can be written as $a_1 + b_1$ where a_1, b_1 are rational numbers with $a_1 < a$ and $b_1 < b$. Similarly, the product $\tau_a \tau_b$ is defined to be the set

$$\tau_{ab} = \{x \in \mathtt{Q} \,|x < ab\} = \{x_1 x_2 | x_1, x_2 \in \mathtt{Q}\,, x_1 < a, x_2 < b\}.$$

In fact one can endow the collection $\{\tau_a | a \in \mathtt{Q}\}$ with *all* the basic properties of $\mathtt{Q}$. So why not try to characterize every point on L by the set of rational numbers to its left? This idea is carried out below (in complete detail) via the device of *Dedekind cuts*.

By a *real number*, we will mean a subset ρ of $\mathtt{Q}$ such that

(i) ρ is neither empty nor all of $\mathtt{Q}$;

(ii) If a is in ρ, then ρ contains every rational number less than a;

(iii) For every a in ρ, there exists a c in ρ such that $a < c$.

A subset ρ defining a real number is often called a *Dedekind cut*, or just a *cut*.

Denote by $\mathtt{R}$ the set of all real numbers. Note that for any rational number a, the singleton set $\{a\}$ is *not* a real number as it does not satisfy (ii) or (iii) above. We have to find another way to put rational numbers inside $\mathtt{R}$.

Note that for any fixed rational number b, the set

$$\tau_b = \{a \in \mathtt{Q} \mid a < b\}$$

is a real number according to the definition above. This way we get a one-to-one mapping

$$\tau : \mathtt{Q} \hookrightarrow \mathtt{R}, \quad b \to \tau_b.$$

Identifying $\mathtt{Q}$ with its image, i.e., not distinguishing between b and τ_b, we may view $\mathtt{Q}$ as a subset of $\mathtt{R}$.

On the other hand, the set

$$\{a \in \mathtt{Q} \mid a \leq b\}$$

is *not* a real number, because property (iii) is not satisfied (for b).

There are infinitely many real numbers which are not rational. For example we have the following

Lemma *Let q be a positive rational number which is not a square in $\mathtt{Q}$. Then the set*

$$\rho_q \; = \; \{a \in \mathtt{Q} \mid a^2 < q \quad or \quad a < 0\}$$

defines a real number.

Proof. Clearly ρ_q is not empty or all of $\mathtt{Q}$, so (i) is satisfied. Now suppose that there exist $a \in \mathtt{Q}$ and b in ρ_q such that $a < b$. We have to show, to get (ii), that a lies in ρ_q. There is nothing to prove if a is negative or zero , so we may assume that a, and hence b, is positive and that a^2 is greater q. But then $b^2 > a^2 > q$ and we get a contradiction to the fact that b belongs to ρ_q. So a must belong to ρ_q.

It is left to prove that (iii) also holds. Pick any a in ρ_q. Since ρ_q obviously contains positive rational numbers, the assertion is clear if a is ≤ 0. So we let a be positive; write it as $\frac{m}{n}$ with $m, n > 0$. Put $t = q - a^2$, which is by definition a positive rational number. For $d \in \mathtt{N}$, put $f(d) = \frac{m^2(d+1)^2}{n^2 d^2} - a^2$. Since $a^2 = \frac{m^2}{n^2}$, $f(d)$ is a positive rational number, and it suffices for us to choose d so that $f(d) < t$, for then $c := \frac{m(d+1)}{nd}$ is a number in ρ_q with $a < c$. But

$$f(d) \; = \; \frac{m^2(2d+1)}{n^2 d^2} \quad \text{and} \quad \frac{2d+1}{d^2} \; < \; \frac{3}{d}.$$

So it suffices to choose d such that $\frac{3}{d}$ is less than $e := \frac{n^2 t}{m^2}$. Since m, n are fixed, so is e. It comes down to picking d to be greater than $3/e$, which is certainly possible. Done.

□

Note that ρ_q^2 identifies with τ_{q^2}, so we may (and we will) think of ρ_q as a square-root of q.

Since $\mathtt{Q} \subset \mathtt{R}$, $\mathtt{R}$ contains 0 and 1.

Theorem $\mathtt{R}$ *admits addition, multiplication and an ordering* $\leq$*, making it a complete ordered field relative to the identities* 0 *and* 1*. Thus the properties* $(\mathcal{R}1) - (\mathcal{R}3)$ *hold in* $\mathtt{R}$*. The property* $(\mathcal{R}4)$ *holds as well.*

Proof. The ordering on $\mathtt{R}$ is obtained by setting

$$\rho \leq \rho' \Leftrightarrow \rho \subset \rho'.$$

We will say that $\rho < \rho'$ iff ρ is a proper subset of ρ'. Clearly, if $\rho \leq \rho'$ and $\rho' \leq \rho$, then $\rho = \rho'$.

First we will prove that the property $(\mathcal{R}4)$ of section 1.1 holds in $\mathtt{R}$. Suppose ρ, ρ' are real numbers such that $\rho < \rho'$. Then by definition, there exists some rational number b in ρ' which is not in ρ. By the property (iii) defining a Dedekind cut, there exists a rational number c in ρ' such that $b < c$. Consequently, we have

$$\rho \ < \ \tau_c \ < \ \rho',$$

where τ_b is the cut representing the rational number b. Done.

Define addition in $\mathtt{R}$ by setting

$$\rho + \rho' \ = \ \{a \in \mathtt{Q} \mid \exists\, b \in \rho, c \in \rho' \quad \text{s.t.} \quad a = b + c\}.$$

It is obvious this operation is commutative and associative. Recall that 0 is represented in $\mathtt{R}$ by $\tau_0 = \{x \in \mathtt{Q} \,|\, x < 0\}$. Therefore, given any $\rho \in \mathtt{R}$ and $b \in \rho$, $b + x$ being $< b$ for any $x < 0$ implies that $\rho + 0 \leq \rho$. Pick any b in ρ. By the property (iii) of any cut, there is some c in ρ such that $b < c$. Then $c - b$ is a positive rational number, and we can find some rational number $-x$ lying strictly between 0 and $c - b$. Then x is negative and $b < x + c$, which implies that b lies in $\rho + 0$. Thus $\rho + 0$ equals ρ. Thus we have the identities $(F1), (F2)$ and $(F7)$.

For any $\rho \in \mathtt{R}$, one defines its *negative* to be

$$-\rho \ = \ \{-a \in \mathtt{Q} \mid a \in \rho^c, \exists\, b \in \rho^c \quad \text{s.t.} \quad b < a\},$$

where ρ^c denotes the complement $\mathtt{Q} - \rho$ of ρ in $\mathtt{Q}$. We will leave it to the reader to check that $-\rho$ is indeed a real number, i.e., that it satisfies properties (i)-(iii) of a cut. We claim that $-\rho + \rho \leq 0$. Suppose not. Then there must

exist $-a$ in $-\rho$ and x in ρ such that $-a + x \geq 0$, i.e., that $a \leq x$. Then by the property (ii), a must belong to ρ, which is a contradiction because by definition a is in ρ^c. Hence the claim.

Suppose $-\rho + \rho$ is strictly less than 0, there must exist a positive rational number y such that $-y$ is not in $-\rho + \rho$. We claim that there exist x in ρ and $-a$ in $-\rho$ such that

$$x + y + a \ = \ 0.$$

We will treat the case when y lies in ρ, and leave the case when it lies in ρ^c as an exercise. Since ρ is not all of $\mathtt{Q}$ and moreover contains all the rationals to the left of any rational it contains, there must exist an $m \in \mathtt{N}$ such that $my \in \rho$, but $(m+1)y \in \rho^c$. By property (iii), there is some rational number q in ρ with $my < q$. If we put $x = q$ and $-a = (m+1)y + (q - my)$, then $x + y + a$ is zero, as desired. Also, since ρ^c contains $(m+1)y$ which is smaller than $-a$, $-a$ is indeed in $-\rho$, and the claim is proved. Consequently, we also have $(F8)$.

Put

$$\mathtt{R}_{>0} \ = \ \{\rho \,|\, \rho > 0\}$$

and

$$\mathtt{R}_{<0} \ = \ \{\rho \,|\, \rho < 0\}.$$

If ρ in $\mathtt{R}$ contains some positive rational number q, it contains all the rationals less than q and so contains τ_0 properly. Thus ρ is positive, i.e., in $\mathtt{R}_{>0}$. Suppose it contains no positive rational number. If it is non-zero, then it is a proper subset of τ_0, i.e., ρ is in $\mathtt{R}_{<0}$, and moreover, its negative $-rho$ will by definition contain a positive rational number and hence lies in $\mathtt{R}_{>0}$. We get $(Ord1)$ and $\mathtt{R}$ is a disjoint union of $\mathtt{R}_{>0}$, $\{0\}$ and $\mathtt{R}_{<0}$. The verification of the remaining *order axiom* $(Ord2)$ is an easy exercise.

Let us now move to *multiplication*. If ρ, ρ' are positive real numbers, we set

$$(-\rho)(-\rho') \ = \ \rho\rho' \ = \ \mathtt{Q}_{<0} \cup \{q \in \mathtt{Q} \,|\, \exists\, a \in \rho \cap \mathtt{Q}_{>0}, b \in \rho' \cap \mathtt{Q}_{>0} \quad s.t. \quad q = ab\}$$

and

$$(-\rho)\rho' \ = \ \rho(-\rho') \ = \ -(\rho\rho').$$

Evidently, this multiplication is commutative and associative, giving $(F3)$ and $(F4)$. It is left to the reader to verify that $\rho\rho'$ is indeed a real number.

We will now check that $\rho \cdot 1$ is ρ. It suffices to deduce this for positive ρ, in which case the inequality $\rho \cdot 1 \leq \rho$ is clear. Also every non-positive a in ρ lies in $\rho \cdot 1$. So let a be a positive rational number in (the cut defining) ρ. By property (iii), $\exists b \in \rho$ with $a < b$. Put $d = a/b$, which is a rational number < 1 and hence belongs to 1, i.e., to τ_1. Hence $a = bd$ lies in $\rho \cdot 1$, and we have $(F6)$. The proof of the *distributivity axiom* is left to the reader to check.

The *multiplicative inverses* for non-zero real numbers is defined as follows: If $\rho \in \mathtt{R}_{>0}$, set

$$\rho^{-1} \;=\; \mathtt{Q}_{\leq 0} \cup \{b \in \mathtt{Q}_{>0} \,|\, b^{-1} \in \rho^c, \exists\, c \in \rho^c \quad \text{s.t.} \quad c < b^{-1}\}$$

and

$$(-\rho)^{-1} \;=\; -(\rho^{-1}).$$

Again the verification that ρ^{-1} is a real number will be left to the reader. Note that ρ^{-1} is also positive. Let a, b be positive rational numbers lying respectively in ρ and ρ^{-1}. Since by definition b^{-1} is in ρ^c, a must be less than b^{-1}. In other words, ab is < 1, which implies that $ab \in \tau_1$. Hence $\rho\rho^{-1} \leq 1$.

Suppose d is an arbitrary rational number in 1. If $d \leq 0$, it will be in $\rho\rho^{-1}$ and we have nothing to do. So assume that d lies strictly between 0 and 1. Suppose d^{-1} lies in ρ. Then, since $d^{-1} > 1$, there must exist some $n \in \mathtt{N}$ such that $d^{-n} \in \rho$, but d^{-n-1} lies in ρ^c. By property (iii) there is some e in ρ such that $d^{-n} < e$. Put $x = d^{-1}e$, which by virtue of being larger than d^{-n-1}, lies in ρ^c. It is easy to check that x^{-1} lies in ρ^{-1}. Hence $d = ex^{-1}$ lies in $\rho\rho^{-1}$, and we get $\rho\rho^{-1} = 1$, establishing $(F9)$.

Thus we have verified that $\mathtt{R}$ is an ordered field containing $\mathtt{Q}$ and satisfying $(\mathcal{R}1), (\mathcal{R}2)$ and $(\mathcal{R}4)$. It remains to prove that $\mathtt{R}$ is a *complete* ordered field, i.e., verify $(Cord)$, which is the same (for $\mathtt{R}$) as $(\mathcal{R}3)$.

Let X be a bounded set of real numbers. Put

$$\beta \;=\; \{a \in \mathtt{Q} \,|\, \exists\, \rho \in X \quad \text{s.t.} \quad a \in \rho\}.$$

Properties (i) and (ii) defining a real number are immediate. For property (iii), note that if $a \in \beta$, then by definition $a \in \rho$ for some $\rho \in X$, and since ρ is a real number, there is some b in ρ such that $a < b$. But then b will also belong to β. So β is a real number.

It is clear that β is an upper bound for X. Suppose γ is another upper bound. Then γ will contain every rational number which occurs in any $\rho \in X$.

Then γ will necessarily contain every rational number occurring in β. So we get $\beta \leq \gamma$, proving that β is indeed the *least upper bound*.

□

It turns out that $\mathtt{R}$ is essentially the only complete ordered field, the reason for which will not be given here. To be precise we have the following

Theorem *Suppose K is a complete ordered field. Then there is a one-to-one correspondence*

$$f : K \to \mathtt{R},$$

which is compatible with the arithmetical operations on both sides, i.e., $f(0) = 0$, $f(1) = 1$, $f(a+b) = f(a) + f(b)$, and $f(ab) = f(a)f(b)$, for all a, b in K.

1.7 Absolute Value

Given any non-zero real number ρ, we can define its *sign*, denoted $\mathrm{sgn}(\rho)$, to be $+$ (or $+1$) if it is positive, and $-$ (or -1) if it is negative.

Define a function

$$|\,.\,| : \mathtt{R} \to \mathtt{R}$$

by setting

$$|0| = 0$$

and for $\rho \neq 0$,

$$|\rho| = \mathrm{sgn}(\rho)\rho.$$

We will call $|\rho|$ the *absolute value* of ρ.

Proposition *The following hold for all ρ, ρ' in $\mathtt{R}$:*

(a) $$|\rho| \geq 0$$

(b) $$|\rho\rho'| = |\rho|.|\rho'|$$

and

(c) $$|\rho + \rho'| \leq |\rho| + |\rho'|.$$

The inequality (c) is called the *triangle inequality*, signifying that the length of any side of a triangle is less than or equal to the sum of the lengths of the other two sides.

Proof. By definition, if ρ is positive, $|\rho|$, resp. $|-\rho|$, is ρ, resp. $-\rho$, whence (a). The assertion (b) is easy, so we will concentrate on (c). If ρ and ρ' have the same sign, or if one of them is zero, we see that $|\rho+\rho'|$ simply equals $|\rho|+|\rho'|$. So let us assume that they are both non-zero *and* have opposite sign. Interchanging ρ and ρ' if necessary, we may assume that ρ is positive and ρ' is negative. Write $\rho' = -\rho_1$, so that ρ_1 is positive and $|\rho|+|\rho'|$ is $\rho+\rho'$. So we need to show that

$$|\rho - \rho_1| \leq \rho + \rho_1,$$

for positive ρ, ρ_1. The left hand side is $\rho - \rho_1$ if $\rho_1 \leq \rho$, in which case the assertion is clear. So let ρ be less than ρ_1. Then the left hand side is $\rho_1 - \rho$, and again the assertion is clear.

□

1.8 Complex Numbers

From here on, we will begin to denote real numbers with letters like $x, y, z, \ldots$ near the end of the (Roman) alphabet, instead of the Greek ones. Note that the definitions we gave in section 1.5 are such that for every non-zero real number x, its square $x^2 = x \cdot x$ is always positive. Consequently, $\mathtt{R}$ does not contain the square roots of any negative number. This is a serious problem which rears its head all over the place.

It is a non-trivial fact, however, that any positive number has two square roots in $\mathtt{R}$, one positive and the other negative; the positive one is denoted $\sqrt{x}$. One can show that for any x in $\mathtt{R}$,

$$|x| = \sqrt{x \cdot x}.$$

So if we can somehow have at hand a square root of -1, we can find square roots of any real number.

This motivates us to declare a new entity, denoted i, to satisfy

$$i^2 = -1.$$

One defines the set of *complex numbers* to be

$$\mathtt{C} = \{x + iy \,|\, x, y \in \mathtt{R}\}$$

and defines the basic arithmetical operations in $\mathtt{C}$ as follows:

$$(x+iy) \pm (x'+iy') \;=\; (x \pm x') + i(y \pm y'),$$

and

$$(x+iy)(x'+iy') \;=\; (xx'-yy') + i(xy'+x'y).$$

There is a natural one-to-one function

$$\mathtt{R} \;\to\; \mathtt{C},\; x \to x + i.0,$$

compatible with the arithmetical operations on both sides.

It is an easy exercise to check the field axioms $(F1)-(F8)$ for $\mathtt{C}$. To get the remaining $(F9)$, however, one has to give an argument. To this end one defines the *complex conjugate* of any $z = x + iy$ in $\mathtt{C}$ to be

$$\overline{z} \;=\; x - iy.$$

Clearly,

$$\mathtt{R} \;=\; \{z \in \mathtt{C} \,|\, \overline{z} = z\}.$$

If $z = x + iy$, we have by definition,

$$z\overline{z} \;=\; x^2 + y^2.$$

In particular, $z\overline{z}$ is either 0 or a positive real number. Hence we can find a non-negative square root of $z\overline{z}$ in $\mathtt{R}$. Define the *absolute value*, sometimes called *modulus* or *norm*, by

$$|z| \;=\; \sqrt{z\overline{z}} \;=\; \sqrt{x^2+y^2}.$$

If $z = x + iy$ is not 0, we will put

$$z^{-1} \;=\; \frac{\overline{z}}{z\overline{z}} \;=\; \frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}.$$

It is a complex number satisfying

$$z(z^{-1}) \;=\; z\frac{\overline{z}}{z\overline{z}} \;=\; 1.$$

Thus $(F9)$ holds in $\mathtt{C}$ as well. Moreover, it is straightforward to check that the Proposition of section 1.6 holds for the absolute value on $\mathtt{C}$. Hence $\mathtt{C}$ is a *field with an absolute value*, just like $\mathtt{R}$.

It is natural to think of complex numbers $z = x + iy$ as being ordered pairs (x, y) of real numbers. So one can try to visualize $\mathbb{C}$ as a plane with two perpendicular coordinate directions, namely giving the x and y parts. Note in particular that 0 corresponds to the origin $O = (0, 0)$, 1 to $(1, 0)$ and i with $(0, 1)$.

Addition of complex numbers has then a simple geometric interpretation: If $z = x+iy$, $z' = x'+iy'$ are two complex numbers, represented by the points $P = (x, y)$ and $Q = (x', y')$ on the plane, then one can join the origin O to P and Q, and then draw a parallelogram with the *line segments* OP and OQ as a pair of adjacent sides. If R is the fourth vertex of this parallelogram, it corresponds to $z + z'$. This is called the *parallelogram law*.

Complex conjugation corresponds to *reflection* about the x-axis.

The *absolute value* or *modulus* $|z|$ of a complex number $z = x + iy$ is, by the Pythagorean theorem applied to the triangle with vertices $O, P = (x, y)$ and $R = (x, 0)$, simply the *length*, often denoted by r, $\sqrt{x^2 + y^2}$ of the line OP.

The *angle* θ between the line segments OR and OP is called the *argument* of z. The pair (r, θ) determines the complex number z. Indeed High school trigonometry allows us to show that the coordinates of z are given by

$$x = r\cos\theta \quad \text{and} \quad y = r\sin\theta,$$

where cos (or cosine) and sin (or sine) are the familiar trigonometric functions. Consequently,

$$z = r(\cos\theta + i\sin\theta).$$

Those who know about *exponentials* (to be treated later in the course) will recognize the identity

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

This can also be taken as a definition of $e^{i\theta}$.

Note that $e^{i\theta}$ has absolute value 1 and hence lies on the *unit circle* in the plane given by the equation $|z| = 1$.