VIII : Set theory as a foundation for mathematics

This material is basically supplementary, and it was not covered in the course. In the first section we discuss the basic axioms of set theory and the desirability of making the axiom system as simple and irredundant as possible. The main objective of the second section is to describe exactly how one can simplify our assumptions for set theory, with particular attention to our fairly lengthy set of axioms for number systems; it turns out that one can replace these by a single assumption that is far more concise and is also central to the basic logical consistency issues raised in the previous unit. In the third section we prove results stated in Unit **V** about the essential uniqueness of number systems satisfying our axioms for the integers and the real number system. The fourth and final section covers a topic that fits in with both the naïve and formal approaches. In Unit **I** of these notes we mentioned that the axioms for Euclidean geometry were viewed as a major portion of the logical foundations for mathematics up to the early 19th century, and that by the end of that century set theory was quickly evolving into a new logical basis for the subject. One natural question is whether the axioms for classical Euclidean geometry can be integrated into the new framework for mathematics, and if so the next question is how this can be done. In the final section we explain how one can view the classical axiomatic approach to geometry within the environment of set theory.

VIII. 1 : Formal development of set theory

(Halmos, §§ 1 – 10, 14; Lipschutz, § 1.12)

In Section **II.1** we began by describing set theory from a naïve viewpoint and then indicated how one could set things up more formally. In most of the notes, our approach has been very much on the naïve side; usually we have introduced assumptions about set theory as they were needed to continue or expedite the discussion without worrying too much about how one should express everything in a completely rigorous manner. This allowed us to develop the subject fairly rapidly. At some points we mentioned the need to be more specific about some issues (***e.g.*,** describing the "admissible" logical statements that can be used to describe sets) or the possibility of deriving some of our assumptions as logical consequences of the others. For example, in Section **III.2** of the notes we mentioned that the existence of objects with the properties of ordered pairs can be proved from the other assumptions; details appear on pages 23 – 25 of Halmos. Frequently the proofs of such implications are somewhat complicated and unmotivated and the approach may seem artificial, and therefore we have simply added assumptions in Section **III.2** and elsewhere to save time and to focus attention on points that are directly related to the uses of set theory in the mathematical sciences.

However, once the basics of set theory have been covered and assimilated, there are some extremely compelling reasons to look back and examine the assumptions in order to see if they can be simplified and redundant assumptions can be eliminated.

One major reason to look for simpler and more concise assumptions is a basic principle in the philosophy of science called ***Ockham's razor*****,** which was originally stated by William of Ockham (1285 – 1349). In modern language, this principle states that

complications should not be introduced unless they are necessary

or in more imperative terms

do not invent unnecessary entities to explain something.

Since we shall appeal to Ockham's razor at other points in this unit, we include an online reference to a biography for William of Ockham**:**

http://plato.stanford.edu/entries/ockham/

In the mathematical sciences there are important practical justifications for using Ockham's razor that go well beyond simplicity of exposition. Since the mathematical sciences are so heavily dependent upon deductive logic, it is absolutely essential to have some assurance that the basic assumptions are logically sound. If the assumptions for some theory lead to logical contradictions, serious questions arise about the validity and reliability of the theory's conclusions and value. ***Simplified lists of basic assumptions turn out to be extremely useful for testing the logical soundness of a mathematical system.*** The reason is obvious; there are fewer things to verify, for much of the work is redirected into verifying the original assumptions are equivalent to the simplified ones.

The advantages of simplified lists of assumptions are also illustrated very clearly by examples within mathematics itself. In mathematical proofs by contradiction, the underlying idea for proving **P** implies **Q** is to assume that **P** is true, to add an assumption that **Q** is false, and to use the new, longer set of hypotheses to obtain a contradiction. This method has a fundamental implication***: As lists of assumptions become longer and more complicated, one must be increasingly careful in checking whether the entire list of assumptions is logically consistent.*** It is generally much easier to check shorter systems of axioms for consistency than it is to check longer ones, so if we want to understand the consistency properties of our axioms it is highly desirable to have an equivalent version which is as simple as possible.

Summary of the basic axioms

As noted in Unit **VII,** one standard axiomatic approach to set theory in present day mathematics is based upon axioms introduced by E. Zermelo during the first decade of the 20th century, with a few subsequent modifications due to other mathematicians, most notably A. Fraenkel. Versions of most ***Zermelo – Fraenkel* (ZF) *axioms*** have been introduced in previous units, and all the other assumptions we have introduced turn out to be consequences of these axioms, all of which are listed below:

- The Axiom of Extensionality (see Section **II.1**)
- The Axiom of Pairs (see Section **II.2** and also below)

- The Axiom of Specification (see Section **II.2**)
- The Axiom of the Power Set (see Section **III.3**)
- The Axiom of Unions (see Section **III.3**)
- The Axiom of Replacement (see Section **IV.4**)
- The Axiom of Foundation (see Section **III.5**)
- The Axiom of Number Systems (see Sections **V.1** and **V.4** as well as the next paragraph)

Note that the Axiom of Choice is missing from this list; if this is added, one obtains the system called **ZFC** in the previous unit. Since a few of the **ZF** axioms have not yet been formulated explicitly, we shall explain the latter in more detail. Given two objects **a** and **b,** the ***Axiom of Pairs*** formally states the existence of the set we have called **{a, b}.** A close inspection of the underlying logical principles reveals a need to make such an assumption in addition to the Axioms of Specification and Unions; in particular, something like this is needed to ensure that sets actually exist in our abstract logical system. The ***Axiom of Number Systems*** is actually not in the usual version of **ZF,** but it represents our assumption that the integers and real number systems are sets; much of this unit will be devoted to discussing the drastically simplified version of this axiom which is part of the usual **ZF** axioms.

As noted in Section **VII.5,** our formulation of set theory in these notes is based on a variant of **ZF** that is due to von J. Neumann, P. Bernays and K. Gödel and called **NBG;** this formulation is closely related to **ZF** and is perhaps the most widely used (although this is generally not stated explicitly outside of mathematical writings on set theory and the foundations of mathematics). One major feature in the latter is its use of **classes** for collections that are too large to be sets; in **ZF** these are not regarded as legitimate objects of any sort. Another important difference is that the Axiom of Specification is simplified in a significant manner. As noted earlier, both formulations yield the same logical consequences, and one is logically consistent if and only if the other is.

We have already given a few online references for the usual axioms of set theory. Here is one more:

http://mathworld.wolfram.com/Zermelo-FraenkelAxioms.html

VIII.2 : Simplified axioms for the basic number systems

(Halmos, §§ 11 – 13)

Units **II** through **VII** covered the basic material in set theory that is needed to use the latter in the mathematical sciences, and this section discusses two basic issues. One, which has already been discussed at some length, concerns the logical consistency problems that follow from Gödel's Incompleteness Theorem. The other is to replace our fairly lengthy set of axioms for the real number system by something that is more concise but logically equivalent. We have already noted the important relationship between these two issues in the preceding section.

The logical consistency problem for set theory

As we have already stated, the logical incompleteness results of Gödel imply that we can never be completely sure that any "reasonable" system of axioms for set theory like **ZF** (Zermelo – Fraenkel) is logically consistent. However, by the relative consistency results of Gödel that we have also discussed, neither the Axiom of Choice nor the (Generalized) Continuum Hypothesis is a potential source of consistency problems. In view of all these results, it is natural to ask where such potential difficulties might lie. There are many similarities between the Axiom of Choice and the Axiom of Foundation; both seem reasonable and both make it easier to discuss some mathematical topics, but both are basically *nonconstructive existence statements*. One further similarity is that there are Gödel relative consistency results for both the Axioms of Foundation and Choice: *If the standard* **ZFC** *axioms for set theory are logically inconsistent, then the system* **ZF** *without the Axiom of Choice is also logically inconsistent. Furthermore, if* **ZF** *is logically inconsistent, then* **ZF** *without the Axiom of Foundation is also logically inconsistent.*

Among the remaining axioms, the next natural candidates are those dealing with something that is infinite. There are two axioms of this type in **ZF,** one of which is the *Axiom of Infinity* — which assumes the existence of an infinite set — and the *Axiom of Specification* — which is really an ***infinite*** (in fact, countably infinite) ***list of axioms*****,** one for each of the admissible statements that can be used to define a set. In our setting, one can prove rigorously that if there is an internal contradiction in the **ZF** axioms for set theory, it must arise either from

(1) the assumptions about constructing sets with definitions given by fairly general types of valid mathematical statements, or from

(2) the assumptions about the existence of the real numbers and its standard hierarchy of subsystems including the natural numbers (nonnegative integers), the (signed) integers and the rational numbers.

Problems concerning the first point arose at the end of the 19th century and the beginning of the 20th century, and two of these are the previously mentioned paradoxes of B. Russell and C. Burali – Forti. We have already noted that mathematicians and logicians resolved these problems by suitably restricting the class of admissible grammatical statements for specifying sets and by adding an axiom which guarantees, among other things, that a set cannot be a member of itself. All of this has now been in place and in its current form for over three quarters of a century. During the intervening time, no additional problems involving the first point have arisen; of course, there are no guarantees that new difficulties will never emerge. However, the absence of new problems over 75 years of intense critical study of foundational questions and enormous progress in all areas of the mathematical sciences lead to an important subjective conclusion: The current Axiom of Specification is highly reliable even if we cannot be sure it is absolutely perfect. Confidence in this respect is reinforced by the **NBG** formulation of set theory due to von Neumann, Bernays and Gödel that we discussed in Section **VI I.5.** The crucial feature of **NBG** is that ***the latter reduces the Axiom of Specification to a* FINITE *list of assumptions at the expense of assuming the existence of "proper classes" that are not sets.***

As noted in Section **VII.5,** even if some new problems eventually arise, most if not all mathematicians strongly believe that they can be handled effectively, although this could very well take a considerable amount of time and effort. It does not seem likely that such repairs would have much effect on most of the mathematics that is currently known, and it is even less likely that there would be any real effect on the applications of the subject (but there might be exceptions for subjects like modern theoretical physics which rely particularly heavily on mathematical ideas). However, we can never be absolutely certain of this.

We now turn to the second point regarding our axioms for number systems. ***Given the numerous assumptions we have made about the real number system, one* MUST NOT *simply ignore the possibility that they could be manipulated to derive a logical contradiction.*** Of course, many of the assumptions about algebraic equations and inequalities are quite standard, and many are just refinements of the simple assumptions (the "common notions") at the beginning of Euclid's ***Elements*.** However, there are two aspects of the axioms for the real numbers that are especially problematic:

A. The existence of infinite sets (for example, the real numbers) is assumed.

B. There is a strong assumption about the existence of least upper bounds that is far less elementary than the other assumptions on equations and inequalities and goes beyond the standard properties of arithmetic operations and inequalities. Formally, **this is another example of a nonconstructive existence statement.**

The standard axioms for set theory

Since the existence of infinite number systems is absolutely central to mathematics, it should be clear that we cannot avoid making some assumption about the existence of an infinite set. A major goal of this section is to indicate how one can use such an axiom to prove the existence of a system which satisfies all the properties we assumed for the real number system. Once this is done, we can use the principle of Ockham's razor to simplify out axioms for set theory to the following:

1. The axioms listed in the preceding section, ***except*** for the Axiom of Number Systems, which is related to the Standard Axiom of Infinity.

2. A simply stated ***Standard Axiom of Infinity*,** which is given below.

3. The ***Axiom of Choice*** or an equivalent statement (***e.g.*,** the Well – Ordering Property or Zorn's Lemma).

Here is the formal statement of the axiom mentioned in the second point on the list:

STANDARD AXIOM OF INFINITY. *There is a set* ω *such that the following hold:*

(1) *The empty set* $\emptyset$ *belongs to* ω.

(2) *For each* $x \in \omega$, *we also have* $x \cup \{x\} \in \omega$.

(3) *If* **A** *is an arbitrary subset of* ω *satisfying the preceding two conditions when* ω *is replaced by* **A**, *then* $A = \omega$.

This axiom corresponds to a model for the nonnegative integers in which $\emptyset$ corresponds to 0 and $x \cup \{x\}$ corresponds to $x + 1$, and the axiom merely says that ***this specific infinite class is a set.***

We can check directly that this set ω satisfies Peano Axioms, with $\sigma(x) = x \cup \{x\}$, as follows: If $y = \sigma(x)$ for some x, then $x \in y$ and hence y is nonempty. Therefore the empty set cannot be equal to $\sigma(x)$ for any x. Next, we need to show that σ is $1 - 1$. Suppose however that $\sigma(x) = \sigma(y)$. Then we have $x \cup \{x\} = y \cup \{y\}$, If x and y are unequal this can only happen if $x \in y$ and $y \in x$; but the Axiom of Foundation implies that these cannot both be true, and this forces us to conclude that $x = y$, so that σ is $1 - 1$. Finally, if M is a subset of ω which contains $\emptyset$ and such that $x \in M$ implies $\sigma(x) \in M$, then the third condition in the Standard Axiom of Infinity implies $M = \omega$. ■

In claiming that the simplified axiom list given above is adequate to yield everything we have done in these notes, we are asserting in particular that

> ***the existence of an object with all the properties of the real number system exists under these assumptions.***

The remainder of this section will explain why this is true. The basic idea is to ***construct a system satisfying all the properties of the real numbers*** using the simplified axiom list in which the assumption on ω replaces the Axiom of Number Systems. We shall not attempt to include all the details; most turn out to be fairly routine arguments, but the work is often tedious. Instead, our main emphasis will be to explain the ideas in the construction. Here are some online references which cover the details in an extremely thorough manner.

http://www.math.nus.edu.sg/~urops/Projects/RealNumbers.pdf

http://www.math.ku.dk/~kiming/courses/2004/matm/real_numbers.pdf

The first reference covers everything, and the second concentrates on Cantor's construction of the real numbers which is described below.

Showing the existence of a object with all the properties of the real number system requires the following preliminary steps:

1. It is necessary to construct the arithmetic operations and linear ordering on the standard model for the Peano axioms.
2. It is necessary to construction of the (signed) integers from the standard model for the Peano axioms.
3. It is necessary to construct the rational numbers from the integers.
4. It is necessary to construct the real numbers from the rationals.

We shall consider each of these in the order listed.

Arithmetic operations, linear ordering and the Peano axioms

Before we can think of constructing the integers or anything else that is larger than the natural numbers N, we need to define addition and multiplication on an abstract system satisfying the Peano axioms and verify that they have the usual properties. The

following recursive definitions of addition, multiplication, and exponentiation are standard, and in particular they appear on page 51 of Goldrei.

(1) **ADDITION** $n + k$: $n + 0 = n$ *and* $n + \sigma(k) = \sigma(n + k)$.

(2) **MULTIPLICATION** $n \times k = n \cdot k$: $n \cdot 0 = 0$ *and* $n \cdot \sigma(k) = (n \cdot k) + n$.

(3) **EXPONENTIATION** $n^k = n\text{^}k$ (*provided* $n \neq 0$) : $n\text{^}0 = 1$ *and* $n\text{^}\sigma(k) = (n\text{^}k) \cdot n$. (*If* $n = 0$, *then we define* $0\text{^}k = 0$ *for all* $k \neq 0$).

The familiar basic arithmetic rules for these operations are stated in Theorem 3.12 on page 53 of Goldrei. These include the commutative and associative laws of addition and multiplication, the distributive law, and the three standard laws of (integral) exponents:

$(m \cdot n)\text{^}k = (m\text{^}k) \cdot (n\text{^}k)$, $(n\text{^}a)\text{^}b = n\text{^}(a \cdot b)$, $(n\text{^}a) \cdot (n\text{^}b) = n\text{^}(a + b)$

Further arithmetic rules appear on pages 53 – 56; most of these are identities for special cases when **n** or **k** is equal to 0 or 1.

The definition of inequality is very easy in this standard model for the Peano axioms; namely, $n < m$ if and only if $n \in m$. The basic properties of inequalities (***e.g.,*** for unequals added to or multiplied by equals) are stated in Theorem 3.13 on page 56, with some further properties listed on the next page.

Construction of the (signed) integers and rational numbers

If one thinks as the (signed) integers as an extension of the natural numbers to allow arbitrary subtraction and the rational numbers as an extension of the integers to allow division by a nonzero integer, it is not surprising that the construction of the integers from the natural numbers and the construction of the rational numbers from the integers should be similar.

Construction of the integers. It is useful to begin by stating exactly what we need to do. Using the existence of a Peano system we are supposed to construct a set $\mathbf{Z}$ together with binary operations $A : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ and $M : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ that correspond to addition and multiplication respectively, we are also supposed to construct a linear ordering on $\mathbf{Z}$, and finally we are supposed to show that these three operations satisfy the properties that were listed in Section $\mathbf{V.2}$.

We have already stated that we want the integers to be a system in which subtraction is always possible, and the key idea in the construction is to start with ordered pairs of natural numbers that we shall think of as formal difference expressions. Of course, two difference expressions $a - b$ and $c - d$ may yield the same number, so we need to identify two difference expressions that yield the same value. It is a very easy exercise in algebra to see that $a - b = c - d$ is true if and only if $a + d = b + c$; the second equation is meaningful within the natural numbers, so we can state our condition for formal differences to be the same using a binary relation given by a subset of $\mathbf{N} \times \mathbf{N}$:

Definition. Two elements **(a, b)** and **(c, d)** of $\mathbf{N} \times \mathbf{N}$ are ***formal difference equivalent*** if $a + d = b + c$.

The name of the relation suggests that formal difference equivalence should be an equivalence relation, and in fact this is true. The proof is a fairly straightforward exercise. As on page 32 of Goldrei, we may now ***define*** the integers $\mathbf{Z}$ to be ***the set of all equivalence classes of this equivalence relation.*** There is a natural embedding of $\mathbf{N}$ into $\mathbf{Z}$ given by sending **n** to the equivalence class of **(n, 0).**

The next step is to define addition, multiplication and ordering on $\mathbf{Z}$ so that it extends the given definitions on $\mathbf{N}$**.** It is easy to guess what sorts of properties the correct definitions should have.

Provisional definitions. Suppose we are given integers **x** and **y** with representatives **(a, b)** and **(c, d)** respectively. Then the sum **x + y** should be represented by the ordered pair **(a + c, b + d),** the product $\mathbf{x \cdot y}$ should be represented by the more complicated ordered pair **(ac + bd, bc + ad),** and the strict linear ordering **x < y** should be equivalent to **a + d < b + c.**

One fundamental issue with this providional definition is that the ***output is given by choosing representatives for the equivalence classes*** **x** and **y.** Since we want functions that are single valued, we need to show that any other choices of representatives for the equivalence classes will yield the same element of $\mathbf{Z}$**.** In standard mathematical terms, ***we must show that our constructions of addition, multiplication and ordering are*** **well – defined***.* This required verifying the three items in the following statement.

Well – definition of operations. *In the notation above, suppose that* **(p, q)** *and* **(a, b)** *represent the same element of* $\mathbf{Z}$**,** *and likewise that* **(r, s)** *and* **(c, d)** *represent the same element of* $\mathbf{Z}$**.** *Then each of the following pairs also represent the same element of* $\mathbf{Z}$**:**

- *The pairs* **(a + c, b + d)** *and* **(p + r, q + s).**
- *The pairs* **(ac + bd, bc + ad)** *and* **(pr + qs, qr + ps).**
- *The inequality* **a + d < b + c** *is true if and only if* **p + s < q + r** *is true.*

Verifying the preceding statements requires a series of elementary but fairly tedious calculations; these are all carried out in the first online document cited above.

The preceding defines addition, multiplication and ordering for the integers, and the next steps are to show that the definitions extend the ones for $\mathbf{N}$ and have all the required properties listed in Section $\mathbf{V.1.}$ Once again, the details may be found in the first online document in our list. The verifications are elementary but somewhat tedious; the standard advice is that "every mathematician should go through the details once and understand them, but not worry about committing them to memory."

Construction of the rational numbers. We are now ready to discuss the construction of the rational numbers from the integers. This is done on pages 29 – 31 of Goldrei with some motivation on page 28.

As we have already noted, the construction of the rational numbers from the integers is supposed to allow division by nonzero quantities, and following the previous construction we begin by considering ordered pairs of integers (with the second one nonzero) to be formal quotients. This is slightly different from the approach in Goldrei,

where the denominator is assumed to be positive, but one ultimately obtains the same system regardless of whether the denominators are assumed to be positive or merely to be nonzero.

One standard condition for two ratios of integers **a/b** and **c/d** to be equal is **ad = bc.** One may use this to define rational numbers using ordered pairs of integers **(x, y)** such that the second term is nonzero, and saying that two elements **(a, b)** and **(c, d)** of the set $\mathbf{Z} \times (\mathbf{Z} - \{0\})$ are ***formal quotient equivalent*** if $\mathbf{a \cdot d = b \cdot c}$.

The name of the relation suggests that formal quotient equivalence should be an equivalence relation, and in fact this is true. The proof is a fairly straightforward exercise. As on page 29 of Goldrei, we may now ***define*** the rational numbers $\mathbf{Q}$ to be ***the set of all equivalence classes of this equivalence relation.*** There is a natural embedding of $\mathbf{Z}$ into $\mathbf{Q}$ given by sending the integer **a** to the equivalence class of $\mathbf{(a, 1)}$.

We can now formulate provisional definitions for addition, multiplication and ordering. The underlying idea is the same as for the construction of the integers, but the formulas will be much different. Suppose we are given rational numbers **x** and **y** with representatives **(a, b)** and **(c, d)** respectively. Then the sum **x + y** should be represented by the ordered pair **(ad + bc, bd),** the product $\mathbf{x \cdot y}$ should be represented by the more complicated ordered pair **(ac, bd),** and the strict linear ordering **x < y** should be equivalent to $\mathbf{abd^2 < b^2cd}$. — Since the latter differs from Goldrei and is clearly more complicated than anything else in sight, we should explain it. A ratio **u/v** will be positive if and only if the product of the numerator and the denominator is positive, and **a/b < c/d** should hold if and only if the difference **(c/d) – (a/b)** is positive. The latter fraction is equivalent to **(bc – ad)/bd,** and the product of this fraction's numerator and denominator is simply $\mathbf{b^2cd - abd^2}$.

In analogy with the construction of integers, the next step is to verify that these constructions do not depend upon the choices of representatives for **x** and **y.** This is covered fairly explicitly on pages 29 – 30 of Goldrei, and because of this and the similarity to the integral case we shall not state all the details here. These are also verified in the first online document cited above, and the advice at the end of the discussion of the integers applies here equally well. One additional point to be checked is that the new definitions of addition, multiplication and ordering coincide with the previous ones on the integers**;** ***i.e.,*** those formal quotients whose denominators are equal to $\mathbf{1}$. This is a tedious but extremely simple exercise, and the argument contains no surprises.

To complete the discussion of the rational numbers, we need to show that they have the standard fundamental properties along the lines of Unit $\mathbf{V}$. Specifically, these include all the properties of the real numbers except the Dedekind Completeness Property.

The Dedekind construction of the real numbers

At certain points when it was necessary for ancient Greek mathematicians to compare irrational numbers, this was done using an idea essentially due to Eudoxus of Cnidus (408 – 355 B.C.E.), which we state in modern language**:**

Condition of Eudoxus. *Two real numbers* **x** *and* **y** *are equal if and only if the following two statements hold.*

(1) *Every rational number less than* **x** *is also less than* **y.**
(2) *Every rational number greater than* **x** *is also greater than* **y.**

One proves this result as follows: If **x** and **y** are unequal, say **x < y,** then there is a rational number **b** between them, and this rational number **b** is greater than **x** but less than **y.** Similar considerations apply if **x > y.** ■

In particular, the Condition of Eudoxus plays an important role in the theory of irrational geometric proportions as developed in Euclid's ***Elements*.**

During the late 1850s, R. Dedekind took these ideas one important step further. For each real number **a,** the set of all rational numbers that are less than **a** has some easily stated properties, and Dedekind's idea was that a converse was true; namely, a set of rational numbers which looks like it could be a set defined by a number actually arises from a real number. The treatment on pages 8 – 17 of Goldrei is slightly different from Dedekind's in some respects, but it is closely related and yields an equivalent object. For the sake of completeness, here is a reference to a readily available book which contains Dedekind's fundamental (and still very readable) paper, ***Continuity and irrational numbers.***

> R. Dedekind, ***Essays on the Theory of Numbers*** (Authorized Translation by W. Beman). Dover, New York, 1963. ISBN: 0–486–21010–3.

Later in this unit we shall indicate how ***Dedekind's approach to the real numbers depends very substantially on being able to work effectively with infinite sets.***

In order to proceed , we need to formalize the notion of "a set of rational numbers which looks like it could be a set defined by a number" in the preceding paragraph. The following definition appears on page 9 of Goldrei.

Definition. A nonempty set **S** of rational numbers is a ***left Dedekind set*** (or the ***left half of a Dedekind cut***) if it has the following properties:

1. The set **S** has an upper bound.
2. The set **S** has no largest element.
3. If **x < y** and **y ∈ S,** then **x ∈ S.**

Strictly speaking, a left Dedekind cut consists of **two** sets, one of which is given above and the other, the right half, is the relative complement. Every rational number **q** determines a left Dedekind set, which is merely the set of all rational numbers that are less than **q.** Verifying the three conditions for such a set is a straightforward exercise.

In Dedekind's approach, one **defines** the real numbers to be the collection of all left Dedekind sets; the axioms of set theory will then imply that this collection is a set.

The next step is to define addition, multiplication and ordering for left Dedekind sets. It is particularly easy to define ordering, for it corresponds to set – theoretic inclusion. With this definition, the important Dedekind Completeness Property follows very quickly; in

fact, the ***least upper bound*** of a bounded collection of left Dedekind sets turns out to be the ***union*** of these sets (see Goldrei, Theorem 2.2, pages 13 – 14).

Defining addition is a little less trivial but still not difficult. Given two left Dedekind sets **C** and **D**, the *sum* **C + D** is taken to be the set of all rational numbers expressible as **x + y** where **x** $\in$ **C** and **y** $\in$ **D.** One needs to check that this is again a left Dedekind set, but this can be done. It is also useful to describe the negative of a left Dedekind set **C** at this point. Let $\mathbf{B_0}$ denote the complement of **C** in the rational numbers, and take **B** equal to $\mathbf{B_0}$ if the latter has no least element **m** and $\mathbf{B = B_0 - \{m\}}$ otherwise; finally define the ***negative*** **– C** to be the set of all numbers **x** such that **– x** $\in$ **B.**

CLAIM: *The set* **– C** *is a left Dedekind set.*

Proof. The first thing to note is that this set is nonempty, or equivalently that **B** is nonempty. The first two conditions on **C** imply that $\mathbf{B_0}$ is nonempty, so all that remains is to verify that $\mathbf{B_0}$ contains more than its least element. In fact, if **m** is the least element and **z** > **m,** then we claim that **x** $\in$ $\mathbf{B_0}$**,** for otherwise we would have **z** $\in$ **C,** and therefore the third property would imply **m** $\in$ **C,** which we know is false.

We shall now verify the three characterizing properties in order. **(1)** Observe that if **y** is any element of **C** then **y** is a lower bound for the sets $\mathbf{B_0}$ and **B;** to see this, suppose that **x** $\in$ $\mathbf{B_0}$ and that **y** is not strictly less than **x.** Then we have **x** $\leq$ **y,** and by the defining properties of **C** it will follow that **x** $\in$ **C,** which contradicts the construction of $\mathbf{B_0}$ as a set that is disjoint from **C.** It therefore follows that **– y** is an upper bound for **– C. (2)** For each **x** $\in$ **– C** we need to find some **y** such that **y** $\in$ **– C** and **y** > **x.** By definition, if we have **x** $\in$ **– C** then **– x** $\in$ $\mathbf{B_0}$ but **– x** is not the least element of the latter. If $\mathbf{B_0}$ has no least element then clearly there is some **w** $\in$ **B** such that **w** < **– x.** If $\mathbf{B_0}$ has a least element we have to look more carefully. Suppose that **w** lies between the least element **m** and **– x;** we claim that **w** $\in$ **B.** If not, then we must have **w** $\in$ **C,** and by the third condition in the definition of a left Dedekind set it will follow that **m** $\in$ **C,** which is false. Therefore in both cases we have an element of **B** such that **w** < **– x ,** and consequently we also have **x** < **– w** where both of the latter belong to **– C.** Hence the latter has no largest element. **(3)** If **x** < **y** and **y** $\in$ **– C,** then we need to prove that **x** $\in$ **– C.** By construction we know that **– y** $\in$ **B,** and of course we also have **– y** < **– x,** so the proof reduces to showing that **– x** $\in$ **B.** What are the other possibilities? One option is that **– x** could be the least element of $\mathbf{B_0}$**,** but this is not true because it is greater than **– y** and the latter lies in **B.** Thus the only remaining alternative to **– x** $\in$ **B** is that we have **– x** $\in$ **C.** Since **– x** > **– y** it would follow that **– y** would lie in **C** and we know this is false because **– y** actually lies in the disjoint subset **B.** Therefore the only possibility is that **– x** $\in$ **B,** which is equivalent to **x** $\in$ **– C.** *This completes the proof that the set* **– C** *is a left Dedekind set.*■

The general definition of multiplication is more complicated. However, if we are given two sets **C** and **D** that are ***positive*** in the sense that both contain $\mathbf{0}$ (hence also contain some positive rational numbers), the definition is again simple: The *product* of the sets

C · D is then taken to be the set of all rational numbers expressible as **x · y** where **x ∈ C** and **y ∈ D.** In the remaining cases one must adjust the definition; this is explained thoroughly on page 15 of Goldrei, and it simply corresponds to the usual rules for determining whether the product of two numbers is positive, negative or zero if at least one of the factors is nonpositive. We specifically took the trouble to define the negative of a left Dedekind set explicitly so that the notion could be used in the definition of multiplication.

Having defined the algebraic structure on left Dedekind sets, it remains to verify that the ordering and algebraic operations satisfy all the properties that are supposed to hold for the real numbers. These are listed in Theorem 2.3 on page 16 of Goldrei. Once again, the first online document cited above has all the details.

The Cantor construction of the real numbers

Given the fundamental importance of the real numbers in mathematics, it certainly would not hurt to confirm the existence of such a system by describing another construction. The standard alternative to Dedekind's construction is the so – called ***Cauchy sequence construction*** due to Cantor. Both yield systems satisfying the axioms for the real numbers, and by the uniqueness results in Section 3, the systems obtained by the different methods are the same for all mathematical purposes. Each approach to constructing the real number system has its own advantages and disadvantages. Some constructions or proofs that are simple and natural in one are difficult or awkward in the other. In particular, the definition of multiplication is much easier in Cantor's construction, but one does not need to worry about equivalence classes in Dedekind's construction, which defines real numbers directly as subsets of the rationals.

The starting point for Cantor's construction is slightly different to the basic idea exploited by Dedekind; namely, *every real number is the limit of a sequence of rational numbers.* There are several ways one can see this, and the standard representations by (usually) unending decimal expansions provide a particularly direct means of doing so (see Section **V.5** of these notes).

Cantor's construction of the real numbers is described on pages 17 – 24 of Goldrei. In order to begin, one needs to define a type of sequence that looks like it should have a limit; the precise concept is called a ***Cauchy sequence***, and it is defined on page 18 **(*Note:*** On page 17, Goldrei notes that every Cauchy sequence of real numbers converges to a limit and describes this as "a dull observation" — not everyone would agree with this opinion, and regardless of whether or not one agrees with it, the result itself and its numerous generalizations are extremely important for many purposes**)**. Sequences whose values are constant and equal to some fixed rational number are Cauchy sequences, and they yield an embedding of the rationals into the set of equivalence classes of Cauchy sequences. One then defines a notion of equivalence if the sequences approach each other asymptotically, after which one defines addition, multiplication and ordering as on pages 22 – 23 of Goldrei. It follows immediately that these operations correspond to the ones we already have for rational numbers. Finally, as indicated on page 23 of Goldrei, one proves that the sets of equivalence classes of Cauchy sequences have all the required properties of the real number system, and this completes the proof that Cantor's construction also yields a model for the real numbers.

The preceding discussions of the Dedekind and Cantor constructions of the real numbers are only meant to summarize the latter and to indicate the crucial role of infinite set theory in both approaches. A reader interested in seeing more of the details is urged to consult the listed references.

The roles of the real number constructions

Most books on the theory of functions of a real variable written during the past few decades begin with the axioms for the real number system and proceed to develop the foundations of calculus from that basis. The actual means of construction of the real numbers is unimportant from this viewpoint, and the following quote from page 16 of Goldrei summarizes the situation quite well:

> The methods found in standard real analysis texts **…** never "look inside" any real number, so the fact that a real number has been defined as a set of rationals ceases to be relevant.

Although the method of construction for the real numbers is relatively unimportant once the process is finished, both the Dedekind and Cantor methods are useful for studying certain other types of questions about embedding one mathematical system in another, where the latter has some desired properties; usually these involve adjoining additional points so that certain "good" sequences will have limits. Such constructions occur frequently in mathematics and its applications (particularly to physics), and they are characterized by names such as ***envelopes, extensions, compactifications, limiting objects,*** or (the default term) ***completions.***

We conclude this discussion of the real numbers with another quotation taken from pages 16 – 17 of Goldrei, which summarizes the preceding discussion and relates it to the material at the end of Section **V.2:**

> It is relevant to note at what cost we have defined the real numbers. First, we have defined reals in terms of rational numbers. **…** Secondly, the definition of an individual real number is as an infinite set of rationals. Use of the infinite in mathematics has been a matter of controversy for a good 2000 [*actually, more like 2500*] years [*in* ***Western*** *civilization at least – many classical Indian mathematicians were not at all reluctant to discuss such matters*]**.** Arguably mathematicians of the 19th century were confident with what is called a ***potentially*** infinite set, one for which, however (finitely) many elements you have, there is always another available. But in treating an ***actually*** infinite set, like a Dedekind left set of rationals, as a legitimate mathematical object suitable for all sorts of manipulation, seemed somewhat dubious.

Complex numbers and other standard constructions. Once the real numbers are defined, there is no problem defining systems like the complex numbers, the usual coordinate spaces of n – dimensional vectors with real or complex coefficients, or any of the other objects one sees in basic undergraduate mathematics; in fact, all the usual construction go through unchanged.

VIII. 3 : Uniqueness of number systems

In the preceding section we outlined the construction of number systems which satisfy the basic properties of the integers, rational numbers and real numbers using the Standard Axiom of Infinity. The purpose of this section is to provide detailed proof ofthe following uniqueness results for number systems from Unit **V:**

Theorem V.1.6. *Suppose that* **X** *and* **Y** *are sets with notions of addition, multiplication and ordering which satisfy all the conditions for the integers. Then there exists a* ***unique*** **1 – 1** *correspondence from* **h** *from* **X** *to* **Y** *that is an* ***isomorphism*** *in the appropriate sense: For all* **u, v ∈ X** *we have* **h(u + v) = h(u) + h(v), h(u · v) = h(u) · h(v),** *and* **h(u) < h(v)** *if and only if* **u < v.** *The map* **h** *sends the zero and unit of* **X** *to the zero and unit of* **Y** *respectively***.**

Theorem V. 4.4. *Suppose that* **X** *and* **Y** *are sets with notions of addition, multiplication and ordering which satisfy all the conditions for the real number system. Then there exists a* ***unique*** **1 – 1** *correspondence from* **h** *from* **X** *to* **Y** *that is an* ***isomorphism*** *in the appropriate sense: For all* **u, v ∈ X** *we have* **h(u + v) = h(u) + h(v), h(u · v) = h(u) · h(v),** *and* **h(u) < h(v)** *if and only if* **u < v.** *The map* **h** *sends the zero and unit of* **X** *to the zero and unit of* **Y,** *and accordingly it also sends the* "*integers*" *in* **X** *to the* "*integers*" *in* **Y** *(and similarly for the* "*rationals*" *in the appropriate systems)***.**

As indicated in Unit **V,** these results imply that

> ***any statement about the addition, multiplication and ordering of* X *is true about the addition, multiplication and ordering of* Y *and conversely.***

Informally, this means that **X** and **Y** are **"*the same for all practical purposes*."** The significance of this is also noted in Sections **V.1** and **V.4;** if there are two systems that satisfy these axioms such that the properties of addition, multiplication and ordering differed in some nontrivial fashion, then one can and should question ***whether there are different versions of mathematics depending upon which system of is chosen to be the* "integers" *or the* "real numbers."** The uniqueness theorem implies that no such difficulties of this sort exist.

Existence of an isomorphism

As usual with statements about the existence of a unique object, the proof splits into two parts, one to establish existence and the other to establish uniqueness. Therefore our first objective will be to construct an isomorphism from **X** to **Y.** We shall start very formally and write our systems as (X, A_X, M_X, O_X) and (Y, A_Y, M_Y, O_Y), where **A** and **M** denote the respective additions and multiplications and **O** denotes the respective linear

orderings. In this terminology, an isomorphism from **X** to **Y** will denote a $\mathbf{1-1}$ correspondence $\mathbf{f : X \to Y}$ such that for all $\mathbf{u, v \in X}$ we have the following relations:

(1) $\mathbf{f(A_X(u, v)) = A_Y(f(u), f(v))}$. [The mapping **f** is ***additive***.]

(2) $\mathbf{f(M_X(u, v)) = M_Y(f(u), f(v))}$. [The mapping **f** is ***multiplicative***.]

(3) If $\mathbf{(u, v) \in O_X}$, then $\mathbf{(f(u), f(v)) \in O_Y}$. [The mapping **f** is ***order preserving***.]

Formally, we want to prove the following.

Theorem 1. *If* **X** *and* **Y** *are systems satisfying the axioms for either the integers or the real numbers (the same number system in both cases), then there exists an isomorphism* $\mathbf{f : X \to Y}$ *in the sense described above*.

It is an elementary exercise to verify that if **f** defines an isomorphism from **X** to **Y,** then the inverse function $\mathbf{f^{-1}}$ defines an isomorphism from **Y** to **X**. In particular, if **X** is isomorphic to **Y**, then **Y** is isomorphic to **X** and one can simply say that **X *and* Y *are isomorphic*** (to each other).

The constructions of the isomorphisms start with the definition for natural numbers (= nonnegative integers) and the proceeds to its definition for the (signed) integers; in the case of the real numbers, the definition is extended still further, first to the rational numbers and ultimately to the real numbers. The first step in both arguments is the same.

First step. We have already noted that there are (unique) embeddings of the natural numbers — say $\mathbf{e_X}$ and $\mathbf{e_Y}$ — into **X** and **Y** sending zero element $\mathbf{0}$ of $\mathbf{N}$ to the zero elements $\mathbf{0_X}$ and $\mathbf{0_Y}$ of **X** and **Y** respectively and satisfying the basic conditions

$$\mathbf{e_X(\sigma(n)) = e_X(n) + 1_X, \quad e_Y(\sigma(n)) = e_Y(n) + 1_Y}$$

where $\mathbf{1_X}$ and $\mathbf{1_Y}$ are the unit elements of **X** and **Y** respectively. For each $\mathbf{x \in X}$ there is at most one $\mathbf{n \in N}$ such that $\mathbf{x = e_X(n)}$, and therefore we can construct a well-defined function

$$\mathbf{f_1 : e_X(N) \to e_Y(N)}$$

by setting $\mathbf{f_1(e_X(n)) = e_Y(n)}$ for $\mathbf{n \in N}$. By construction this defines a one-to-one correspondence between $\mathbf{e_X(N)}$ and $\mathbf{e_Y(N)}$.

CLAIM*:* The map $\mathbf{f_1}$ satisfies the conditions

$$\mathbf{f_1(A_X(u, v)) = A_Y(f_1(u), f_1(v)),}$$

$$\mathbf{f_1(M_X(u, v)) = M_Y(f_1(u), f_1(v)),}$$

$$\text{if } \mathbf{(u, v) \in O_X,} \text{ then } \mathbf{(f_1(u), f_1(v)) \in O_Y}$$

for all $\mathbf{u, v \in N}$. Using the maps $\mathbf{e_X}$ and $\mathbf{e_Y}$ we may rewrite these conditions as

$$\mathbf{f_1(A_X(e_X(m), e_X(n))) = A_Y(f_1(e_X(m)), f_1(e_X(n))),}$$

$$\mathbf{f_1(M_X(e_X(m), e_X(n))) = M_Y(f_1(e_X(m)), f_1(e_X(n))),}$$

$$\text{if } (e_X(m), e_X(n)) \in O_X, \text{ then } (f_1(e_X(m)),\ f_1(e_X(n))) \in O_Y$$

for all $m, n \in \mathbf{N}$. We shall verify the first two of these by induction on n; in order to simplify the notation and stress the underlying ideas we shall use the standard algebraic terminology to denote the addition, multiplication and linear orderings on X and Y.

Addition. Suppose that $n = 0$. Then

$$f_1(e_X(m) + e_X(0)) = f_1(e_X(m) + 0_X) = f_1(e_X(m)) = e_Y(m) + 0_Y = e_Y(m) + e_Y(0) = f_1(e_X(m)) + f_1(e_X(0)).$$

Thus the equation is true for $n = 0$ and all m. Suppose now that it is true for $n = k$ and all m; we need to show it is true for $n = \sigma(k)$ and all m. But

$$f_1(e_X(m) + e_X(\sigma(k))) = f_1(e_X(m) + e_X(k) + 1_X) = f_1(e_X(m) + e_X(k) + 1_X) = f_1(e_X(m) + 1_X + e_X(k)) = f_1(e_X(\sigma(m)) + e_X(k))$$

and by the induction hypothesis the last expression is equal to

$$f_1(e_X(\sigma(m))) + f_1(e_X(k)).$$

The latter in turn is equal to

$$e_Y(\sigma(m)) + e_Y(k) = e_Y(m) + 1_Y + e_Y(k) = e_Y(m) + e_Y(\sigma(k)) = f_1(e_X(m)) + f_1(e_X(\sigma(k))).$$

This completes the verification of the inductive step.

Multiplication. Suppose that $n = 0$. Then

$$f_1(e_X(m)\cdot e_X(0)) = f_1(e_X(m)\cdot 0_X) = f_1(0_X) = 0_Y = e_Y(m)\cdot 0_Y = e_Y(m)\cdot e_Y(0) = f_1(e_X(m))\cdot f_1(e_X(0)).$$

Thus the equation is true for $n = 0$ and all m. Suppose that we know the equation is true for $n = k$ and all m; we need to show it is true for $n = \sigma(k)$ and all m. But

$$f_1(e_X(m)\cdot e_X(\sigma(k))) = f_1(e_X(m)\cdot e_X(k) + e_X(m)) = f_1(e_X(m)\cdot e_X(k)) + f_1(e_X(m))$$

because we have already verified that f_1 is additive, and by the induction hypothesis the last expression is equal to $f_1(e_X(m))\cdot f_1(e_X(k)) + f_1(e_X(m))$. The latter in turn is equal to

$$e_Y(m)\cdot e_Y(k) + e_Y(m) = e_Y(m)\cdot e_Y(\sigma(k)) = f_1(e_X(m))\cdot f_1(e_X(\sigma(k))).$$

As before, this completes the verification of the inductive step.

Ordering. If $e_X(m) < e_X(n)$ then there is a nonzero natural number $c \in \mathbf{N}$ such that $e_X(m) + e_X(c) = e_X(n)$. Since f_1 is one-to-one, it follows that $e_Y(c) = f_1(e_X(c)) \neq 0_Y$, so that $e_Y(c) > 0_Y$. By the additivity of f_1 it follows that

$$f_1(e_X(m)) = e_Y(m) = e_Y(m) + 0_Y < e_Y(m) + e_Y(c) = f_1(e_X(m) + e_X(c)) = f_1(e_X(n))$$

as required.

Notational conventions. Let **F** be a system satisfying the axioms for the integers or the real number system, and let $\mathbf{e_F : N \to F}$ be the embedding of the natural numbers that has been used extensively in the preceding step of the proof. We define the **integers** in **F** to be the set of all objects of the form $\mathbf{e_F(a) - e_F(b)}$ for some $\mathbf{a, b \in N}$, and we shall denote this set by $\mathbf{Z(F)}$. Similarly, if **F** satisfies the axioms for the reals, we define the ***rational numbers*** or ***rationals*** in **F** to be the set of **m**/**n** where **m** and **n** are integers in **F** and **n** is nonzero, and we shall denote this set by $\mathbf{Q(F)}$. If we are dealing with one fixed system in a given context we shall omit the "**(F)**" to simplify and standardize the notation.

Second step. We need to extend $\mathbf{f_1}$ to negative integers. Clearly we want a definition sending a negative number of the form $\mathbf{-e_X(n) \in X}$ to $\mathbf{-e_Y(n) = -f_1(e_Y(n))}$, but we shall take a slightly less direct approach that will be helpful in verifying the crucial properties of the extended map without a succession of case by case arguments.

By the preceding definition, every integer $\mathbf{n \in X}$ can be represented as a difference $\mathbf{e_X(a) - e_X(b)}$ for some $\mathbf{a, b \in N}$; this representation is not unique, but it is elementary to check that $\mathbf{e_X(a) - e_X(b) = e_X(c) - e_X(d)}$ if and only if

$$\mathbf{e_X(a) + e_X(d) = e_X(b) + e_X(c).}$$

We shall extend $\mathbf{f_1}$ to a map $\mathbf{f_2}$ on integers by setting

$$\mathbf{f_2\,(e_X(a) - e_X(b)) = e_Y(a) - e_Y(b) = f_1(e_X(a)) - f_1(e_X(b)).}$$

Before proceeding any further we need to show that $\mathbf{f_2}$ is well-defined; in other words, we need to verify that

$$\text{if } \mathbf{e_X(a) - e_X(b) = e_X(c) - e_X(d),} \text{ then } \mathbf{e_Y(a) - e_Y(b) = e_Y(c) - e_Y(d).}$$

Equivalently, we need to show that

$$\text{if } \mathbf{e_X(a) + e_X(d) = e_X(b) + e_X(c),} \text{ then } \mathbf{e_Y(a) + e_Y(d) = e_Y(b) + e_Y(c).}$$

To see the latter, apply $\mathbf{f_1}$ to both sides of the first equation and note that the additivity of $\mathbf{f_1}$ on **N** implies that

$$\mathbf{e_Y(a) + e_Y(d) = f_1(e_X(a)) + f_1(e_X(d)) = f_1(e_X(a) + e_X(d)) = f_1(e_X(b) + e_X(c)) = f_1(e_X(b)) + f_1(e_X(c)) = e_Y(b) + e_Y(c)}$$

so that $\mathbf{f_2}$ is well-defined.

Throughout the remainder of this step in the proof we shall consider two integers in **X** of the form $\mathbf{m = e_X(a) - e_X(b)}$ and $\mathbf{n = e_X(c) - e_X(d).}$

We must now show that $\mathbf{f_2}$ is $\mathbf{1-1.}$ To see this, suppose that $\mathbf{f_2(m) = f_2(n).}$ By construction it follows that $\mathbf{e_Y(a) - e_Y(b) = e_Y(c) - e_Y(d)}$ so that we have $\mathbf{e_Y(a) + e_Y(d) = e_Y(b) + e_Y(c).}$ The identities of the previous paragraph now imply that

$$\mathbf{f_1(e_X(a) + e_X(d)) = f_1(e_X(b) + e_X(c))}$$

and since $\mathbf{f_1}$ is $\mathbf{1-1}$ it follows that $\mathbf{e_X(a) + e_X(d) = e_X(b) + e_X(c).}$ But the latter implies $\mathbf{e_X(a) - e_X(b) = e_X(c) - e_X(d)}$ which in turn implies that $\mathbf{m = n.}$ By construction it

follows that the image of $\mathbf{f_2}$ is the set of all differences of elements in the image of $\mathbf{e_Y}$; in other words, $\mathbf{f_2}$ ***maps the integers in*** **X** ***onto the integers in*** **Y.**

We next verify that $\mathbf{f_2}$ is additive:

$$\mathbf{f_2(m+n) = f_2(e_X(a) - e_X(b) + e_X(c) - e_X(d)) =}$$
$$\mathbf{f_2\,(e_X(a) + e_X(c) - e_X(b) - e_X(d)) = f_2\,((e_X(a) + e_X(c)) - (e_X(b) + e_X(d))) =}$$
$$\mathbf{f_1(e_X(a) + e_X(c)) - f_1(e_X(b) + e_X(d)) = (e_Y(a) + e_Y(c)) - (e_Y(b) + e_Y(d)) =}$$
$$\mathbf{e_Y(a) - e_Y(b) + e_Y(c) - e_Y(d) = f_2(m) + f_2(n).}$$

The verification that $\mathbf{f_2}$ is multiplicative proceeds similarly:

$$\mathbf{f_2(m \cdot n) = f_2\,((e_X(a) - e_X(b)) \cdot (e_X(c) - e_X(d))) =}$$
$$\mathbf{f_2((e_X(a) \cdot e_X(c) + e_X(b) \cdot e_X(d)) - (e_X(a) \cdot e_X(d) + e_X(b) \cdot e_X(c))) =}$$
$$\mathbf{f_1(e_X(a) \cdot e_X(c) + e_X(b) \cdot e_X(d)) - f_1(e_X(a) \cdot e_X(d) + e_X(b) \cdot e_X(c)) =}$$
$$\mathbf{(f_1(e_X(a)) \cdot f_1(e_X(c)) + f_1(e_X(b)) \cdot f_1(e_X(d))) -}$$
$$\mathbf{(f_1(e_X(a)) \cdot f_1(e_X(d)) + f_1(e_X(b)) \cdot f_1(e_X(c))) =}$$
$$\mathbf{(e_Y(a) \cdot e_Y(c) + e_Y(b) \cdot e_Y(d)) - (e_Y(a) \cdot e_Y(d) + e_Y(b) \cdot e_Y(c)) =}$$
$$\mathbf{(e_Y(a) - e_Y(b)) \cdot (e_Y(c) - e_Y(d)) = f_2(m) \cdot f_2(n).}$$

To prove that $\mathbf{f_2}$ is order preserving, suppose that $\mathbf{m < n,}$ so that we have

$$\mathbf{e_X(a) - e_X(b) < e_X(c) - e_X(d).}$$

Adding $\mathbf{e_X(b) - e_X(d)}$ to both sides of this inequality yields

$$\mathbf{e_X(a) + e_X(d) < e_X(b) + e_X(c)}$$

and since $\mathbf{f_1}$ is order preserving the latter in turn implies

$$\mathbf{e_Y(a) + e_Y(d) = f_1(e_X(a)) + f_1(e_X(d)) = f_1(e_X(a) + e_X(d)) <}$$
$$\mathbf{f_1(e_X(b) + e_X(c)) = f_1(e_X(b)) + f_1(e_X(c)) = e_Y(a) + e_Y(c).}$$

If we now subtract $\mathbf{e_Y(b) + e_Y(d)}$ from both sides of the outside inequality we obtain the desired conclusion:

$$\mathbf{f_2(m) = e_Y(a) - e_Y(b) < e_Y(c) - e_Y(d) = f_2(n)}$$

This completes the second step of the proof.

Note that the preceding two steps complete the proof of Theorem **V.1.6.**■

Third step. We may now assume that **X** and **Y** satisfy the axioms for the real numbers, so that we need an extension of $\mathbf{f_2}$ to rational numbers of the form $\mathbf{a/b}$ where **a** and **b** are integers and **b** is nonzero. Recall from elementary algebra that two fractions $\mathbf{a/b}$ and $\mathbf{c/d}$ (with **b** and **d** nonzero) are equal if and only if $\mathbf{ad = bc.}$

The idea is to consider a number $\mathbf{q \in X}$ of the form $\mathbf{a/b,}$ where **a** and **b** are integers in **X** and **b** is nonzero, and to define $\mathbf{f_3(q) = f_2(a)/f_2(b).}$ In order to show that this is a valid definition we need to check two things. First of all, since $\mathbf{f_2}$ is $\mathbf{1-1}$ it follows that $\mathbf{f_2(b)}$ is nonzero if **b** is nonzero, so the quotient is actually defined. Second, we need to show that the value obtained by the formula is the same if we write **q** as a quotient of integers

in two different ways. In other words, we need to show that if $\mathbf{a/b = c/d}$ (with **b** and **d** nonzero) then we also have $\mathbf{f_2(a)/f_2(b) = f_2(c)/f_2(d)}$. To do this, begin with the previous observation that **ad = bc** and apply $\mathbf{f_2}$ to both sides of the equation to obtain $\mathbf{f_2(a)\cdot f_2(d) = f_2(b)\cdot f_2(c)}$. If we then divide both sides of this equation by $\mathbf{f_2(b)\cdot f_2(d)}$ we obtain the desired equation $\mathbf{f_2(a)/f_2(b) = f_2(c)/f_2(d)}$.

By construction the image of $\mathbf{f_3}$ consists of all expressions of the form **u** / **v** where **u** and **v** are in the image of $\mathbf{f_2}$ and **v** is nonzero; in other words, $\mathbf{f_3}$ **maps the rationals in X onto the rationals in Y.** We claim that $\mathbf{f_3}$ is $\mathbf{1-1}$.

Throughout the remainder of this step in the proof we shall consider two rational numbers in **X** of the form **p = a/b** and **q = c/d** where **a, b, c, d** are integers in **X** and **b** and **d** are nonzero.

To prove that $\mathbf{f_3}$ is $\mathbf{1-1}$, suppose that $\mathbf{f_3(p) = f_3(q)}$. By construction it follows that $\mathbf{f_2(a)/f_2(b) = f_2(c)/f_2(d)}$, which is equivalent to $\mathbf{f_2(a)\cdot f_2(d) = f_2(b)\cdot f_2(c)}$. Since $\mathbf{f_2}$ is multiplicative we have $\mathbf{f_2(ad) = f_2(a)\cdot f_2(d) = f_2(b)\cdot f_2(c) = f_2(bc)}$, and since $\mathbf{f_2}$ is one-to-one this implies **ad = bc,** which in turn implies **a/b = c/d** and hence that ***the mapping*** $\mathbf{f_3}$ ***is also*** $\mathbf{1-1}$.

The ***verification that*** $\mathbf{f_3}$ ***is additive*** is a consequence of the following string of equations:

$$f_3\left(\frac{a}{b}+\frac{c}{d}\right)=f_3\left(\frac{ad+bc}{bd}\right)=\frac{f_2(ad+bc)}{f_2(bd)}=\frac{f_2(a)\,f_2(d)+f_2(b)\,f_2(c)}{f_2(b)\,f_2(d)}=$$

$$\frac{f_2(a)}{f_2(b)}+\frac{f_2(c)}{f_2(d)}=f_3\left(\frac{a}{b}\right)+f_3\left(\frac{c}{d}\right).$$

Similarly, the ***verification that*** $\mathbf{f_3}$ ***is multiplicative*** follows from a somewhat different string of equations:

$$f_3\left(\frac{a}{b}\cdot\frac{c}{d}\right)=f_3\left(\frac{ac}{bd}\right)=\frac{f_2(ac)}{f_2(bd)}=\frac{f_2(a)\,f_2(c)}{f_2(b)\,f_2(d)}=$$

$$\frac{f_2(a)}{f_2(b)}\cdot\frac{f_2(c)}{f_2(d)}=f_3\left(\frac{a}{b}\right)\cdot f_3\left(\frac{c}{d}\right).$$

Finally we need to ***show that*** $\mathbf{f_3}$ ***is order preserving.*** We shall do this using the fact that a fraction **a/b** is positive if and only if the product of the number and denominator **ab** is positive (the second number is the product of the first with the positive number $\mathbf{b^2}$). Therefore suppose that **p < q;** then **p – q** is positive, and by the observation on the signs of fractions in the previous sentence it follows that the integer $\mathbf{(bc-ad)\cdot bd}$ is also positive. Since $\mathbf{f_2}$ is order preserving it follows that

$$\mathbf{f_2((bc-ad)\cdot bd) = (f_2(b)\cdot f_2(c) - f_2(a)\cdot f_2(d))\cdot(f_2(b)\cdot f_2(d))}$$

is also positive. But the right hand side of this equation is equal to $f_3(q) - f_3(p)$, so the preceding observations imply that $f_3(q) > f_3(p)$ as required.

Fourth step. We need to extend f_3 to all elements of X. Given a number $r \in X$, consider the set $D(r)$ of all rational numbers $q \in X$ such that $q < r$. Let k be a positive integer that is greater than r, and consider the set $f_3[D(r)] \subset Y$. Since f_3 is order preserving it follows that $f_3(k)$ is an upper bound for $f_3[D(r)]$ and therefore by completeness the set $f_3[D(r)]$ has a (unique) least upper bound; we take $f(r)$ to be this least upper bound. This definition may be rewritten as follows:

$$f(r) = \text{L.U.B.}_{q < r}\ f_3(q)$$

The first order of business is to show that $f_3(r) = f(r)$ when r is rational. If r is rational and $q \in D(r)$, then by the previous work we know that $f_3(q) < f_3(r)$, so that $f_3(r)$ is an upper bound for $f_3[D(r)]$ and consequently is greater than or equal to the least upper bound, which is $f(r)$. Suppose now that $f(r) < f_3(r)$. It follows that there is a rational number $t \in X$ such that $f(r) < f_3(t) < f_3(r)$. Since f_3 is order preserving, the second inequality implies that $t < r$. The latter in turn implies $t \in D(r)$ and hence $f_3(t) \leq f(r)$, which when combined with the previously displayed inequality $f(r) < f_3(t)$ yields a contradiction. It follows that $f(r) = f_3(r)$.

To ***show that*** f ***is*** $1-1$, assume that r and s are real numbers in X such that $r < s$. Choose rational numbers p and q such that $r < p < q < s$. As before, it follows that $f_3(p)$ is an upper bound for $f_3[D(r)]$ and therefore we have $f(r) \leq f_3(p) = f(p)$. Furthermore, since $f_3 = f$ for rational numbers it follows that $f(p) < f(q)$, and also since $q \in D(s)$ it follows that $f(q) = f_3(q) \leq f(s)$. If we put these inequalities together we find that $f(r) < f(s)$ and consequently that f ***is also*** $1-1$. Note that ***this argument also shows that*** f ***is order preserving.***

We shall next ***verify that the function*** f ***maps*** X ***onto all of*** Y. Let $y \in Y$ be arbitrary, and let $D^*(y)$ be the set of all rational numbers $q \in Y$ such that $q < y$; by construction y is an upper bound for $D^*(y)$, and in fact y is the least upper bound of $D^*(y)$ because if $z < y$ then there is a rational number p such that $z < p < y$. As before there is a positive integer $k \in Y$ such that $y < k$, and since the function f_3 is order preserving it follows that $k_0 = f_3^{-1}(k)$ is an upper bound for the set $f_3^{-1}[D^*(y)]$. Therefore the latter set has an upper bound that we shall denote by x. We claim that $f(x) = y$, and we shall do this by showing that $y \leq f(x)$ and strict inequality does not hold. To show the inequality, suppose that we have $q < y$, and choose a rational number $p \in Y$ such that $q < p < y$. If we write $q_0 = f_3^{-1}(q)$ and $p_0 = f_3^{-1}(p)$ then $q_0 < p_0$, and since both belong to the set $f_3^{-1}[D^*(y)]$ it follows that $q_0 < p_0 < x$. Since the function f is order preserving the identities $p = f_3(p_0) = f(p_0)$ and $q = f_3(q_0) = f(q_0)$ imply the chain of inequalities $q < p < f(x)$. Thus $f(x)$ is an upper bound for $D^*(y)$; since y is the least upper bound for $D^*(y)$, we must have $y \leq f(x)$. The proof that $y = f(x)$ thus reduces to showing that $f(x)$ is ***not*** strictly greater than y.

Assume the contrary. Then there is a rational number **q** satisfying $y < q < f(x)$, and write $q = f_3(q_0) = f(q_0)$ as before. Since the function **f** is order preserving, it follows that $q_0 < x$. But the definition of **x** as a least upper bound implies the existence of a rational number p_0 such that $q_0 < p_0$ and $p = f_3^{-1}(p_0)$ lies in $D^*(y)$; ***i.e.***, we must have $p < y$. Once again we have $q = f_3(q_0) < f_3(p_0) = p$, and if we combine this with the other inequalities, we get the longer string of inequalities $y < q < p < y$, which is a contradiction. This completes the proof that $y = f(x)$.

The next step is to ***show that*** **f** ***is additive.*** Let **u** and **v** be arbitrary real numbers in **X.**

Consider first the special case where one of these numbers (say **v**) is rational. In this case the set $D(u + v)$ is the set of all numbers expressible as sums

$$f_3(q) + f_3(v) = f_3(q) + f(v)$$

where $q \in D(u)$, and therefore we have

$$f(u + v) = \text{L.U.B.}_{q < u + v}\ f_3(q) = \left[\text{L.U.B.}_{p < u}\ f_3(p)\right] + f(v) = f(u) + f(v)$$

and hence **f** is additive if **v** is rational and **u** is arbitrary.

We now consider the general case. If **q** is a rational number such that $q < v$, then we have $f(u) + f(q) = f(u + q) < f(u + v)$ because **f** is order preserving and it is also additive if one of the summands is rational. Therefore $q < v$ implies that

$$f_3(q) = f(q) < f(u + v) - f(u)$$

and consequently we have

$$f(v) = \text{L.U.B.}_{q < v}\ f_3(q) \leq f(u + v) - f(u).$$

Additivity will follow if we can show that $f(v) < f(u + v) - f(u)$ is impossible, so assume that it does hold. In this case there is a rational number $r \in Y$ such that

$$f(v) < r < f(u + v) - f(u)$$

and because **f** is onto we may write $r = f(q)$ for some rational number $q \in X$. Since **f** is order preserving we know that $v < q$, and consequently the order preserving and partial additivity properties of **f** imply that

$$f(q) = r < f(u + v) - f(u) < f(u + q) - f(u) = f(u) + f(q) - f(u) = f(q)$$

which is a contradiction. Therefore the assumption $f(v) < f(u + v) - f(u)$ must be incorrect, and by the preceding discussion it follows that **f** must be additive.

At this point, ***the only statement that remains to be shown is that*** **f** **is multiplicative.** We first observe that **f** is multiplicative if at least one of the factors is 0 or ± 1. If one of the factors is $+1$, this is immediate because $f(1_X) = 1_Y$. If one of the factors is zero, this follows quickly because the product of anything with zero is zero and $f(0_X) = 0_Y$. If one of the factors is -1, this will follow provided we can demonstrate that $f(-a) = -f(a)$ for all $a \in X$, for then we have $f(-1_X) = -f(1_X) = -1_Y$ and furthermore

$$f((-1_X)\cdot a) = f(-a) = -f(a) = (-1_Y)\cdot f(a) = f(-1_X)\cdot f(a).$$

To see that $f(-a) = -f(a)$, let $b = -a$. Since **f** is additive we have that

$$0_Y = f(0_X) = f(a + b) = f(a) + f(b)$$

and the latter implies that $f(b) = -f(a)$ as required. We are going to need the basic identity $f(-a) = -f(a)$ in order to complete the final step in the verification that **f** is multiplicative.

The next step in verifying that* f *is multiplicative is to show this is true if both of the factors are positive. The proof of this fact is very similar to the proof of additivity (since the exponential map defines an order preserving isomorphism from the additive group of real numbers to the multiplicative group of positive real numbers, this should not be surprising). Let **u** and **v** be arbitrary ***positive*** real numbers in **X.** Since **f** is order and zero preserving it follows that both $f(u)$ and $f(v)$ are positive.

Consider first the special case where one of these numbers (say **v**) is rational (and positive!). In this case, the set $D(u \cdot v)$ is the set of all real numbers expressible as sums $f_3(q) \cdot f_3(v) = f_3(q) \cdot f(v)$ where $q \in D(u)$, and therefore we have

$$f(u \cdot v) = \text{L.U.B.}_{\,q < u \cdot v}\ f_3(q) = [\,\text{L.U.B.}_{\,p < u}\ f_3(p)\,] \cdot f(v) = f(u) \cdot f(v)$$

and hence **f** is multiplicative if **v** is rational and **u** is arbitrary.

We now consider the general case. If **q** is a rational number such that $q < v$, then we have $f(u) \cdot f(q) = f(u \cdot q) < f(u \cdot v)$ because **f** is order preserving and it is also additive if one of the summands is rational. Therefore $q < v$ implies that

$$f_3(q) = f(q) < f(u \cdot v)/f(u)$$

and consequently we have

$$f(v) = \text{L.U.B.}_{\,q < v}\ f_3(q) \leq f(u \cdot v)/f(u).$$

Multiplicativity will follow if we can show that $f(v) < f(u \cdot v)/f(u)$ is impossible, so assume that it does hold. In this case there is a rational number $r \in Y$ such that

$$f(v) < r < f(u \cdot v)/f(u)$$

and because **f** is onto we may write $r = f(q)$ for some rational number $q \in X$. Since **f** is order preserving we know that $v < q$, and consequently the order preserving and partial multiplicativity properties of **f** imply that

$$f(q) = r < f(u \cdot v)/f(u) < f(u \cdot q)/f(u) = f(u) \cdot f(q)/f(u) = f(q)$$

which is a contradiction. Therefore the assumption $f(v) < f(u \cdot v)/f(u)$ must be incorrect, and by the preceding discussion it follows that **f** must be multiplicative.

Finally, ***we need to verify that* f *is multiplicative in all cases.*** Given a nonzero real number **a,** set $\varepsilon(a)$ equal to $+1$ if **a** is positive and -1 if **a** is negative. Then we may express $a = \varepsilon(a) \cdot |a|$ where the absolute value $|a|$ is positive. Using the multiplicativity of **f** for the product $|u| \cdot |v|$ and the identity $f(\varepsilon \cdot a) = \varepsilon \cdot f(a)$ for $\varepsilon = \pm 1$ we have

$$f(u \cdot v) = f\,((\varepsilon(u) \cdot |u|) \cdot (\varepsilon(v) \cdot |v|)) = f\,(\varepsilon(u) \cdot \varepsilon(v) \cdot |u| \cdot |v|) =$$
$$(\varepsilon(u) \cdot \varepsilon(v)) \cdot f(|u| \cdot |v|) = (\varepsilon(u) \cdot \varepsilon(v)) \cdot f(|u|) \cdot f(|v|) =$$
$$(\varepsilon(u) \cdot f(|u|)) \cdot (\varepsilon(v) \cdot f(|v|)) = (f(\varepsilon(u) \cdot |u|)) \cdot (f(\varepsilon(v) \cdot |v|)) = f(u) \cdot f(v)$$

and this completes the proof that **f** is multiplicative. As noted before, this completes the proof of Theorem 1 as well as Theorem **V.4.4.**■

Uniqueness of the isomorphisms

It turns out that the isomorphisms constructed above are **unique.** This is equivalent to saying that if **A** satisfies the axioms for the integers or the real numbers, then ***the only isomorphism of* A *with itself that preserves addition, multiplication and ordering is the identity.*** In fact, a slightly stronger result is true

Theorem 2. *If* **A** *satisfies the axioms for the real numbers or the integers and the mapping* $\mathbf{f: A \to A}$ *is a* $\mathbf{1-1}$ *correspondence that is additive and multiplicative (but is not* ***assumed*** *to preserve the ordering), then* **f** *is the identity.*

It is possible to define meaningful notions of isomorphism for many different classes of mathematical objects. If the domain and codomain of an isomorphism are the same, it is often called an ***automorphism.*** Given an object satisfying the axioms for the real number system, the identity map on that object is always an automorphism, and the main result above can be reformulated to state that for a system satisfying the axioms for the real number system there are no other automorphisms.

Example of a nontrivial automorphism. In contrast, there are some systems closely related to the real number systems that have nontrivial automorphisms. Perhaps the most important example is the field of ***complex numbers*** $\mathbf{C}$**.** Of course, this is the system one obtains from the real numbers by adding an element $\mathbf{i}$ that is supposed to be the square root of $\mathbf{-1}$**.** A detailed account of the complex numbers is really beyond the scope of these notes, but the book by Birkhoff and MacLane covers the basics in a clear, concise and thorough manner. Here our interest lies with the ***complex conjugation mapping*** on complex numbers sending a complex number $\mathbf{z = a + bi}$ to its conjugate $\mathbf{\chi(z) = z^* = a - bi}$**.** This is a $\mathbf{1-1}$ correspondence because the identity $\mathbf{z = (z^*)^*}$ implies $\mathbf{\chi\chi = 1_C}$**,** so that χ is its own inverse, and χ is an automorphism because complex conjugation satisfies the following two elementary identities:

$$\mathbf{(z+w)^* = z^* + w^* \qquad\qquad (z \cdot w)^* = z^* \cdot w^*}$$

For the sake of completeness we note that ***the set of all automorphisms of the complex numbers is*** **HUGE** (in fact, its cardinality is $\mathbf{2^{|C|} > |C|}$), but conjugation is the only nontrivial automorphism that sends real numbers to themselves and it is also the only nontrivial one which defines a ***continuous*** mapping from $\mathbf{C}$ to itself.

Proof of Theorem 2. The proof begins with a couple of simple observations:

> **(a)** *The only element* $\mathbf{u \in A}$ *such that* $\mathbf{x \cdot u = x}$ *for all* $\mathbf{x \in A}$ *is the unit element.*
>
> **(b)** *The only element* $\mathbf{z \in A}$ *such that* $\mathbf{x \cdot z = z}$ *for all* $\mathbf{x \in A}$ *is the zero element.*

These follow because $\mathbf{u = 1 \cdot u = 1}$ and $\mathbf{0 = 0 \cdot z = z}$. Since **f** sends elements with properties **(a)** and **(b)** into elements with the corresponding properties, it follows that we must have $\mathbf{f(1) = 1}$ and $\mathbf{f(0) = 0}$.

We shall also need two other standard elementary properties of automorphisms (and isomorphisms):

(c) *For all* $\mathbf{x \in A}$ *we have* $\mathbf{f(-x) = -f(x)}$.

(d) *If* $\mathbf{A = R}$, *then for all nonzero* $\mathbf{x \in A}$ *we have* $\mathbf{f(x^{-1}) = f(x)^{-1}}$.

The proof of **(c)** is the same argument that was used in the uniqueness proof, and the proof of **(d)** is based upon similar considerations:

$$\mathbf{1 = f(1) = f(x\,x^{-1}) = f(x)\,f(x^{-1}) \quad \Rightarrow \quad f(x^{-1}) = f(x)^{-1}}$$

The main idea behind the proof is to show successively that **f** must be the identity on each of the following:

1. The natural numbers.
2. The integers.
3. The rational numbers.
4. All real numbers.

If **A** is the integers, then only the first two steps are needed. Predictably, we take these steps in the order listed.

The natural numbers. Let $\mathbf{e : N \to A}$ be the embedding described in the section on axioms for the real numbers. We shall show that $\mathbf{f(e(n)) = e(n)}$ by induction on **n;** we have already verified this if $\mathbf{n = 0}$ or $\mathbf{n = 1}$. Suppose that this is known for $\mathbf{n = k}$. Then by the additivity of **f** and the inductive hypothesis we have

$$\mathbf{f(e(\sigma(k))) = f(e(k) + 1) = f(e(k)) + 1 = e(k) + 1 = e(\sigma(k)),}$$

and hence **f** is the identity on the natural numbers (more correctly, on the image of the natural numbers in the reals).

The integers. Given an integer $\mathbf{n \in Z}$, write $\mathbf{n = e(a) - e(b)}$ where $\mathbf{a, b \in N}$. Then by the preceding step in the proof, the additivity condition and property **(c)** above we have

$$\mathbf{f(n) = f(e(a) - e(b)) = f(e(a)) - f(e(b)) = e(a) - e(b) = n}$$

as required. Note that ***this completes the proof if*** $\mathbf{A = Z}$.

The rational numbers. We may now assume that $\mathbf{A = R}$. Given an arbitrary rational number $\mathbf{q \in Q}$ express **q** as a quotient $\mathbf{a\,b^{-1}}$ where $\mathbf{a, b \in Z}$ and **b** is nonzero. As before, by the immediately preceding step in the proof, the multiplicativity of **f** and property **(d)** above we have

$$\mathbf{f(q) = f(a\,b^{-1}) = f(a)\,f(b^{-1}) = f(a)\,f(b)^{-1} = a\,b^{-1} = q}$$

as required.

The set of all real numbers. The crucial step in the proof is to ***show that*** **f** ***is order preserving.*** Suppose that $\mathbf{a, b \in R}$ satisfy $\mathbf{a > b}$. If $\mathbf{c = a - b}$ then $\mathbf{c > 0}$ and

therefore **c** has a unique positive square root that we shall call **d.** If we apply f to both sides of the equation $\mathbf{d^2 = a - b}$ we obtain the equation

$$\mathbf{f(d)^2 = f(d^2) = f(a - b) = f(a) - f(b);}$$

this quantity is nonzero because **f** is $\mathbf{1 - 1}$ (look at the right hand side), and it is nonnegative because it is a square (look at the left hand side). Therefore the quantity in question is positive as claimed.

To conclude the proof, let $\mathbf{a \in R}$ be arbitrary. We need to show that neither of the strict inequalities **a > f(a)** or **a < f(a)** can hold. The proofs in both cases are similar so we shall do them simultaneously. Suppose that **a > f(a)** or **a < f(a)** is true, and in the respective cases choose a rational number **q** such that

$$\mathbf{a > q > f(a) \quad or \quad a < q < f(a).}$$

Since **f** is order preserving and is the identity on rational numbers, these inequalities respectively imply

$$\mathbf{f(a) > f(q) = q > f(a)} \quad \text{and} \quad \mathbf{f(a) < f(q) = q < f(a).}$$

In either case we obtain a contradiction, and therefore we must have **f(a) = a.** ■

V I I I. 4 : Set theory and classical geometry

In Section **I.2** we noted that classical Euclidean geometry had served as a working foundation for much of mathematics before the development of set theory and the Dedekind – Cantor constructions for the real number system out of the rational numbers. Further discussion of this point appears on pages 212 and 258 – 259 of the following online documents**:**

http://math.ucr.edu/~res/math133/geomnotes5a.pdf

http://math.ucr.edu/~res/math133/geomnotes5b.pdf

We also noted in Section **I.2** that logical difficulties were noticed in the classical setting for geometry (***i.e.*****,** as presented in the ***Elements***) around the same time, but subsequent work near the end of the 19th century put classical geometry into a more logically rigorous form that meets current standards. The purpose of this appendix is to indicate in more detail how classical Euclidean geometry fits into the framework of set theory in modern mathematics. Our purpose is not really to go through the basics of classical Euclidean geometry but rather to explain how one integrates it into modern mathematics. References for further details will be given at appropriate points.

In the ***Elements,*** geometry is developed by starting with some basic assumptions on the properties of space and deriving an extensive list of logical consequences. If we are going to work within set theory, we must formulate the key mathematical aspects of geometry in set – theoretic terms rather than "physical reality." The first step in this process is very simple. A set should be a formal mathematical model for a geometrical plane or **3 –** dimensional space **E ,** and the *points* of the space should be the elements

of **E.** *Lines*, and also *planes* in the $\mathbf{3}$ **–** dimensional case, will then be sets of points and hence subsets of **E;** the geometric concept of a point **x** lying on a line **L** or plane **P** will mean that **x** belongs to **L** or **P** respectively. In the ***Elements,*** both lines and planes are defined intuitively, but from the viewpoint of logic it is necessary to start with some things that are simply given without formal definitions, and therefore the formal set – theoretic approach to geometry takes lines and planes simply as distinguished classes of subsets, nothing more and nothing less. When we study geometry we usually think that these mathematical lines and planes should be idealizations of physical lines and planes, but this intuition serves only as a guide and motivation for our work. To summarize this discussion, the first steps in placing deductive geometry within the framework of set theory is to assume that plane or $\mathbf{3}$ **–** space of classical geometry should be a set **E,** and the additional structure should one or two classes of proper subsets depending upon the dimension. In both cases there is a family of nonempty proper subsets Λ called ***lines,*** and in the $\mathbf{3}$ **–** dimensional case there is also a second family of nonempty proper subsets Π called ***planes*** such that Λ and Π are disjoint.

Clearly we need to make some assumptions; for example, we obvious need to know that two points determining a unique line. Properties of this sort are called ***incidence axioms***, and here are lists of the respective axioms for the plane and $\mathbf{3}$ **–** space.

Planar axioms.

[$\mathbf{I}$ **– 1**] Given two distinct points **x** and **y** in **E,** there is a unique line **L** in Λ such that both $\mathbf{x} \in \mathbf{L}$ and $\mathbf{y} \in \mathbf{L}$.

[$\mathbf{I}$ **– 2**] Every line **L** contains at least two points.

Spatial axioms. – In addition to the previous axioms, also include the following.

[$\mathbf{I}$ **– 3**] Given three distinct points **x, y** and **z** in **E** such that no line **L** contains them all (***i.e.*****,** they are **noncollinear**), there is a unique plane **P** in Π such that $\mathbf{x, y, z} \in \mathbf{L}$.

[$\mathbf{I}$ **– 4**] Every plane **P** contains at least three noncollinear points.

[$\mathbf{I}$ **– 5**] If two points of a line **L** belong to a plane **P,** then the entire line is contained in **P.**

[$\mathbf{I}$ **– 6**] If two planes have one point in common, then they also have a line in common.

The last two axioms correspond to everyday experience about the relation between planes and lines. One can derive various consequences from these assumptions (for example, that two distinct lines have at most one point in common), but we shall not work these out.

We now proceed to the basic measurement concepts in classical geometry; namely, linear and angular measurement. Once again, it is advisable to set things up formally so that at least linear measurement is an undefined concept and at this point it is also better to take both types of measurements as undefined concepts. We have mentioned that *the classical Greek approach to real numbers* was to *view them as lengths of segments*; we shall effectively reverse this approach by ***defining*** *lengths of segments in terms of the real number system*, which we now have at our disposal. Now the length of a segment can also be viewed as the distance between the endpoints, and the principle of Ockham's razor indicates the latter is preferable way of viewing an undefined concept

because it will not require us to digress and explain exactly what a line segment should be. Therefore the "undefined" linear measurement structure will be a a function

$$d : \mathbf{E} \times \mathbf{E} \rightarrow \mathbf{R}$$

that will have several properties, of which these are the most basic:

1. The quantity $d(\mathbf{x}, \mathbf{y})$ is always nonnegative, and it is zero if and only if $\mathbf{x} = \mathbf{y}$.
2. For all **x** and **y** we have $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.

Likewise, at this point we would like to define angle measure in a manner that does not require us to explain exactly what is meant by an angle. Intuitively it is clear that a nontrivial angle (two distinct branch pieces and not a straight angle) is completely determined by 3 noncollinear points such that the middle one is the vertex of the angle. One way of doing this is to start by taking the subset $\mathit{Indep.}(\mathbf{E} \times \mathbf{E} \times \mathbf{E})$ of all ordered triples $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ in $\mathbf{E} \times \mathbf{E} \times \mathbf{E}$ such that **x, y** and **z** are three noncollinear points of **E** (*i.e.*, the three points are *geometrically independent*), and to define angle measurement to be a function

$$\alpha : \mathit{Indep.}(\mathbf{E} \times \mathbf{E} \times \mathbf{E}) \rightarrow (0, 180)$$

which will have some desired properties that we shall not attempt to describe for the time being.

Restriction to the planar case. Henceforth, unless there is an explicit statement to the contrary, we shall focus our attention on classical plane geometry. We have already seen that formulating incidence axioms is a somewhat more complicated in the $3-$ dimensional case. In fact, working everything out in three dimensions is a fairly routine extension of the $2-$ dimensional case; aside from the additional incidence axioms, it is only necessary to make some relatively straightforward adjustments in wording to a few of the axioms. This is not difficult, but the relatively minor differences make it awkward to discuss both cases simultaneously, and concentrating on the simpler case illustrates the basic ideas that arise in both situations.

By the preceding discussion, the data we need to discuss Euclidean plane geometry are the set **E** of points, the family Λ of lines, the linear measurement function d, and the angular measurement function α. Such an approach to axiomatic geometry is called a ***synthetic metric approach.*** The idea is basically due to G. D. Birkhoff (1884 – 1944), and it is described in the two references listed below. These two references differ significantly in content and objectives; the first item is a research paper in which an extremely short list of axioms is stated, and the second is a book which was written to relate Birkhoff's ideas to the content and exposition of standard high school courses in geometry at the time (the book was first published in 1940).

G. D. Birkhoff, A set of postulates for plane geometry (based on scale and protractors), *Annals of Mathematics* (2) **33** (1932), pp. 329 – 345.

G. D. Birkhoff and R. Beatley, ***Basic Geometry*** (3rd Ed.). A. M. S. Chelsea Publishing, Providence, RI, 1999. ISBN**:** 0–821–82101–6

More elaborate (and higher level) accounts of classical geometry based upon Birkhoff's approach appear in the textbook and online site listed below:

E. E. Moise, ***Elementary Geometry from an Advanced Standpoint*** (3rd Ed.). Addison – Wesley, Reading, MA, 1990. ISBN: 0–201–50867–2

http://www.math.uncc.edu/~droyster/math3181/notes/hyprgeom/hyprgeom.html

We shall call the latter ***Royster's online site.***

A brief description of the axioms

We have seen that the axioms for the real number system split naturally into three groups. One set of axioms concerns the basic properties of addition and multiplication, a second set concerns the basic properties of the linear ordering and its relationship to the arithmetic operations, and the third is the Dedekind Completeness Axiom. There is also a division of the axioms for Euclidean plane geometry into several groups. To save time and space, we shall not quote all the axioms precisely. Full statements and further information can be found in the four references cited above as well as the following sources:

E. C. Wallace and S. F. West, ***Roads to Geometry*** (3rd Ed.)**.** Prentice – Hall, Upper Saddle River, NJ, 2003. ISBN: 0–130–41396–8.

http://math.ucr.edu/~res/math153/history03.pdf

1. Incidence axioms.

We have already discussed these.

2. Distance axioms.

We have discussed some simple properties that distance is supposed to satisfy, but the most important properties are summarized in the following strong assumption.

RULER POSTULATE. If **L** is a line, then there is a $\mathbf{1-1}$ correspondence $\mathbf{f : L \to R}$ such that for all $\mathbf{x, y \in L}$ we have $\boldsymbol{d(x, y) = |f(x) - f(y)|}$**.** In other words, with respect to the given notion of distance on the plane, *every line looks like the standard real number line.*

3. Separation axiom.

In order to state this axiom correctly we must make several definitions based upon the structure developed thus far. All this is done explicitly at the online site**:**

http://math.ucr.edu/~res/math153/history03c.pdf

and therefore we shall only explain the key ideas. Using the Ruler Postulate one can formulate a concept of betweenness for an ordered triple of distinct collinear points. The Plane Separation Postulate is an assumption which states that for each line **L,** the points of the relative complement $\mathbf{E - L}$ split into a pair of disjoint subsets, called the ***sides*** or ***(open) half – planes*** in **E** with respect to **L** and these have the expected properties involving betweenness; namely, if two points lie on the same side then every point

between them also lies on that side, and if two points lie on opposite sides, then there is some point of **L** that lies between them.

4. Angular measurement axioms.

It is not possible to write these down formally without introducing numerous definitions based upon all the previous data and assumptions, so we shall simply try to summarize what happens. One needs **(1)** a simple, general criterion for constructing angles with a given measurement in a fairly arbitrary position, **(2)** an assumption that supplementary angles have measurements adding up to **180, (3)** the usual sort of principle for concluding that the measurement of one angle is the sum of the measures of two other angles, and finally **(4)** something relating linear measures to angular measures; a standard way of doing this is to assume the familiar Side – Angle – Side congruence test from elementary geometry, but it is also possible to formulate everything with a simpler underlying assumption.

5. Euclidean Parallel Postuate.

This corresponds to Euclid's Fifth Postulate. For reasons related to Ockham's razor, many mathematicians starting (at least) with Proclus Diadochus (410 – 485) have preferred to take the following statement named after J. Playfair (1748 – 1819), which is logically equivalent to the original Euclid's Fifth Postulate but does not involve linear or angular measurement:

PLAYFAIR'S POSTULATE. Given a line **L** and a point **x** not on **L,** then there is a unique line **M** in the plane determined by **L** and **x** such that $\mathbf{x} \in \mathbf{M}$ but **L** and **M** do not have any points in common (since we are working in a plane, such lines are ***parallel***).

Abbreviated versions of the axioms. Partly because of Ockham's razor, and partly for reasons involving logical consistency like those stated in Section 1, it is useful to find axiomatic systems that are as economical as possible. In his 1932 paper, Birkhoff showed that one could get by with four assumptions that are simple to state but have very strong implications. There is a much different approach to making everything more concise in

http://math.ucr.edu/~res/math153/history03c.pdf

which gives a set of six relatively straightforward axioms that only involve the two "undefined concepts" of lines and distance; in this system it is possible to construct a notion of angular measurement which has all the desired properties. Of course, it is necessary to prove that such a construction is possible under the given assumptions and that the construction satisfies the required conditions. Completing these tasks takes a significant amount of time and effort, and it relies very heavily upon numerous ideas in the following book by H. G. Forder (1889 – 1981)**:**

> H. G. Forder, ***The foundations of Euclidean geometry***
> (Reprint of the original 1927 edition). Dover Books, New York, NY, 1958. ASIN: B0007F8NLG.

One additional advantage of the axiom system described in the online reference is that it adapts very easily to give a set of axioms for the non – Euclidean geometry that was developed in the early 19th century by J. Bolyai (1802 – 1860) and N. Lobachevsky (1792 – 1856), and was also known to C. F. Gauss. All one needs to do is replace the final axiom.

5*. Hyperbolic Parallel Postuate.

There are two versions, but one can prove that they are logically equivalent.

STRONG VERSION. Given a line **L** and a point **x** not on **L,** then there are ***at least two*** lines **M** and **N** such that $x \in M \cap N$ but $L \cap M$ and $L \cap N$ are both empty.

WEAK VERSION. There is ***at least one pair*** **(L, x),** consisting of a line **L** and a point **x** not on the line **L,** for which there are ***at least two lines*** **M** and **N** such that $x \in M \cap N$ but both of the sets $L \cap M$ and $L \cap N$ are empty.

The weak version of the Hyperbolic Parallel Postulate is the formal negation of Playfair's Postulate; namely, the existence of unique parallels fails ***somewhere.*** The strong version says it fails everywhere, and the point of logical equivalence is that ***if Playfair's Postulate fails somewhere then it fails everywhere.*** Of course, this is something that must be proved, and the material in Royster's online site gives the details.

Birkhoff's abbreviated axioms and non – Euclidean geometry. The four Birkhoff axioms in the 1932 paper cannot be simply modified to describe non – Euclidean hyperbolic geometry. The reason for this is related to the final axiom, which is the Side – Angle – Side Similarity Theorem from classical Euclidean geometry. There is no corresponding similarity theory in non – Euclidean geometry, so it is clear that one cannot get a short system of axioms for the latter by some simple changes to the Birkhoff axioms.

Relative consistency models for the axioms

The book by Moise and the online reference by Royster show that one can obtain a complete description of the Euclidean plane or the non – Euclidean hyperbolic plane using the axioms described above. However, this does not quite imply that classical Euclidean geometry can be integrated into set theory. In order to complete the process, we need to show the following**:**

It is possible to construct a system within set theory which satisfies all the conditions for a Euclidean plane that we have described above.

The existence of such an example (or ***model*** *for the axioms*) will also show that the axioms satisfy an important relative consistency test; namely, the axioms for Euclidean geometry are logically consistent if the axioms for set theory are logically consistent. The online document

http://www.math.uiuc.edu/~gfrancis/M302/handouts/postulates.pdf

constructs a system of the desired type, showing that the abbreviated Birkhoff axioms are satisfied. In fact, the construction is based upon the standard coordinate model for Euclidean geometry in which points are interpreted as ordered pairs of real numbers, lines are defined to be the sets of ordered pairs **(x, y)** such that $Ax + By + C = 0$, where *at least one* of **A, B** is nonzero, distance is defined by the usual formula in coordinate geometry, and angle measure measurement is defined by the standard vector formula for the cosine of an angle between to two vectors (note that the standard *Cauchy – Schwarz – Bunyakovsky inequality* in linear algebra implies this algebraically

defined number lies in the interval $[-1, 1]$). Details appear on pages 5 – 7 of the online reference. Algebraic verification of the Birkhoff axioms for these definitions of lines, distance and angle measurement are summarized on pages 5 – 8 of the document cited directly above.■

There is one point in the preceding reference that deserves some thought. The inverse cosine function is of course given in terms of the cosine function, but the usual definition of the latter in trigonometry books is given geometrically. This may raise questions about whether the reasoning described in the preceding paragraph is circular. One way to answer such an objection is to define trigonometric functions, and derive the basic trigonometric identities, by some formal method that does not use Euclidean geometry explicitly (although the reasoning may/will be geometrically motivated at various points). This can be done by ***defining*** the sine and cosine to be equal to the usual power series expansions that are given in calculus and somehow proving that the functions defined by these power series have the expected properties (***e.g.,*** the standard trigonometric equation $\sin^2\theta + \cos^2\theta = 1$, or the formulas for the sine and cosine of a sum of two numbers) without using geometrical arguments. One reference for such a development of the basic trigonometric functions is pages 182 – 184 of the previously cited book by Rudin (***Principles of Mathematical Analysis***). A more elementary discussion along the same lines appears in Appendix **E** of the following book:

> P. Ryan, ***Euclidean and non-Euclidean geometry: An analytical approach.*** *Cambridge University Press,* Cambridge, U. K., and New York, NY, 1986. ISBN: 0–521–27635–7

Relative consistency models for non – Euclidean geometry. One can also prove a relative consistency result for non – Euclidean geometry by constructing set – theoretic models of the corresponding axioms, but both the construction of the model and the verification of its key properties are considerably more difficult than in the Euclidean case. The models, and the verification that they satisfy the axioms, are given by results of E. Beltrami (1835 – 1900), F. Klein (1849 – 1925) and H. Poincaré (1854 – 1912) from the second half of the 19th century.

The existence of such relative consistency models is the basis for assertions that ***the parallel postulate in classical geometry cannot be proven from the other assumptions***. If this were possible, it would contradict the existence of the models discussed in the preceding paragraph. Further discussion about the relative consistency of non – Euclidean geometry can be found on pages 255 – 258 of the following online document:

http://math.ucr.edu/~res/math133/geomnotes5b.pdf

The logical independence of the Euclidean and hyperbolic parallel postulates from the preceding assumptions is analogous to the formal status of the Axiom of Foundation, the Axiom of Choice and the Generalized Continuum Hypothesis that was discussed in the previous unit. However, there is one significant difference, for mathematicians find it convenient to view both axiom systems for geometry as equally valid, but in contexts that do not touch upon the foundations of mathematics it is generally more convenient to stick with a fixed list of axioms for set theory. Generally this is given by **ZFC** or **NBG** plus the Axiom of Choice with no assumption either way about the Generalized Continuum Hypothesis, but as we have noted there are some important exceptions, most notably the viewpoints of ***intuitionism*** and ***constructivism***. A full discussion of

such matters is beyond the scope of these notes, but we shall include a list of online references for both the mainstream view of the foundations of mathematics as well as some of the alternatives:

http://sakharov.net/foundation.html

http://en.wikipedia.org/wiki/Philosophy_of_mathematics

http://en.wikipedia.org/wiki/Foundations_of_mathematics

http://www.rbjones.com/rbjpub/logic/

http://www.math.psu.edu/simpson/hierarchy.html

http://plato.stanford.edu/entries/hilbert-program/

http://en.wikipedia.org/wiki/David_Hilbert#Formalism

http://plato.stanford.edu/entries/logic-intuitionistic/

http://www.math.fau.edu/Richman/HTML/CONSTRUC.HTM

http://en.wikipedia.org/wiki/Constructivism_(mathematics)

http://plato.stanford.edu/entries/mathematics-constructive/

http://www.rbjones.com/rbjpub/philos/maths/faq025.htm

http://www.rbjones.com/rbjpub/philos/maths/faq027.htm

http://www.rbjones.com/rbjpub/philos/maths/faq004.htm

Additional remarks on alternate formulations for the foundations of mathematics (using functions rather than sets as the main building blocks) were made at the beginning of Section **IV.3.**