Undergraduate Research Opportunity Programme in Science

CONSTRUCTION OF THE REAL NUMBER SYSTEM

Submitted by
Gary Sng Chee Hien

Supervised by
A/P Denny Leung Ho-Hon

**Department of Mathematics
National University of Singapore**

Academic Year 2000/2001

ABSTRACT

The real number system is usually taken for granted in even the most basic of real analysis course. This might lead some mathematics majors to graduate with the notion that the real number system is the foundation of mathematics. In fact, the real number system is not really a fundamental system in the sense that it can be created from more basic structures. This project will attempt to show one such construction by starting with the axioms of Peano. Basically, this assumes the existence of a natural number system which can be intuitively accepted. Along the way, the integers, rationals and finally the real numbers will be constructed systematically. The project culminates with the revelation that any complete ordered field is in fact the real number system. Another aim of this project is to present fundamental concepts of mathematics at the undergraduate level in an intuitive manner, and it is hoped that the general readers would gain from this report not only a more through understanding of the familiar real number system, but also appreciate that most mathematical concepts are in fact natural and easily grasped, if only general prejudices against abstractness and mathematical symbols can be set aside. The author sincerely hope that this project can claim to have achieved the second aim.

TABLE OF CONTENTS

INTRODUCTION

Most mathematics undergraduates should be familiar with the real number system. Besides the normal rules of addition and multiplication, we further know that it is a field, possesses the Archimedean property and that it is Cauchy complete. What we may not know is the reason why such properties exist or should exists. If we stop and ponder a bit on the real number system, it would seem that we really do know very little about the real number system, even at an intuitive level. For example, can we visualize a real number that is not rational? How do we relate the real numbers to the more intuitive rationals? Can we perhaps do away with the real number system altogether and stick to the rationals? Is it possible to assume another different type of real number system while preserving all the current results and theorems in mathematics? That is, is the real number system unique?

To answer these questions, it would perhaps be useful if we start at a level that is more fundamental than the real number system. If we can construct the real number system from a more basic structure such as the natural number system, then perhaps the construction process would reveal to us the necessity or reasons behind the existence of some of its fundamental properties. In particular, we may discover the reason why the rationals are not adequate as a real number system. Hopefully, we should be able to tell at the end of the project whether the real number system is logically necessary or just simply a fanciful product of the mathematical mind!

This project attempts to systematically reconstruct the real number system with Peano's axioms as the foundation. There will be no assumption at all of familiar number properties, integer, rational or otherwise. In fact, part of the main occupation of this project is to create systems whose elements demonstrate such properties. This does not mean we are necessarily going to take the hard and tedious approach in our proofs. The definition section will introduce general concepts that are useful to our construction. The general proof section will then prove general results of such concepts that will henceforth be considered part of the reader's basic knowledge and no further justification will be made of such results in the actual construction process. The reason for such an approach is obvious. There are many similarity between the various number systems, and most results can actually be commonly shared. For example, the integer system, field of rationals and the real number system are all ordered integral domain. Instead of proving the properties of the binary operations separately for each system, it would seem wise to establish such properties in a general setting. After all, the proofs would run similar in each case also, since the reason why such properties hold depend not on the particular system but just the fact that it is an ordered integral domain. Also, it helps us see more clearly the difference between the various systems, when we encounter properties that cannot be generalized. Hence, this approach not only saves work but is also more illuminating!

Finally, the author would like to apologize to the mature reader(*A/P Denny Leung, Dr Wong Yan Loi etc*) if this report appear more wordy and frivolous than most mathematical reports. Most likely, the elaboration and comments in the definition section and throughout the construction process are simply redundant reading to a refined mathematical mind. To such readers, the author recommends that only the bolded definitions and theorems portions be formally consulted. But the author would like to use this project to demonstrate that mathematics need not be all that difficult or abstract, and that the symbols and definitions that mathematicians have come up with is not a conspiracy to make life difficult for the average student. Rather, most definitions are motivated by intuitive ideas and the symbols are really shorthand that reduces a 30-page long word proof to a more elegant 1 page proof. It is hoped that the elaboration in words would first capture the attention of the layman and reveal to him the gist and motivation of such concepts. Then perhaps he will eventually make an effort to decode the symbolic technical definition whereby he will obtain a more satisfying and precise idea.

Acknowledgement

The author would like to thank his mentor A/P Denny Leung Ho-Hon for his utmost patience and help throughout this project. He has helped to clarify concepts, suggest alternate approaches to some proofs and has posed questions which makes the project all the more interesting. In particular, his question regarding why exponentiation behaves differently from addition and multiplication in the natural number system still puzzle the author to this day. Even though this project has come to a close, the author hopes to provide a satisfactory answer to that question one day.

The author would also like to show his appreciation to his friend Eveline for helping out with the typing of the report, which ironically turns out to be a more frustrating endeavor than the project itself

DEFINITION SECTION

Set

For the scope of this project, we neither probe into axiomatic set theory nor seek to define what a set is. The 10 axioms of set theory will not be referred to formally. Instead, their basic consequences and properties shall be treated as simple, obvious facts. Any operation with sets will be deal with in a naïve and intuitive manner. Least of all, we assume that there is such a thing as the empty set, that we can form union and intersection of sets, that we know when 2 sets are equal etc. The starting point of the project is the *assumption of the existence* of a set, which we shall call a set of natural numbers, which satisfy the 5 axioms of Peano. In axiomatic set theory, the existence of such a set can and must be proved. It involves construction from more elementary sets postulated in the 10 axioms but as far as this project is concerned, that is another story.

Relation

Given any 2 non-empty sets A and B, a relation, **R**, from A to B is any subset of A×B. If $(a,b)\in\mathbf{R}$, then we write a**R**b. The set

$\{a\in A|(a,b)\in\mathbf{R}$ for some $b\in B\}$

denoted **D**(**R**), is called the **domain** of **R** and the set

$\{b\in B|(a,b)\in\mathbf{R}$ for some $a\in A\}$

denoted **R**(**R**), is called the **range** of **R** for obvious reason. One can view a relation as a mapping from a subset of A onto a subset of B with absolutely no restriction.

In the case that a relation, **R**, is from A to A, we can check whether **R** satisfy the following properties:

(i) Reflexive

$a\mathbf{R}a\ \forall\ a\in A$

(ii) Symmetric

$a_1\mathbf{R}a_2\Rightarrow a_2\mathbf{R}a_1\ \forall\ a_1,a_2\in A$

(iii) Transitive

$a_1\mathbf{R}a_2$ and $a_2\mathbf{R}a_3\Rightarrow a_1\mathbf{R}a_3\ \forall\ a_1,a_2,a_3\in A$

(iv) Anti-symmetric

$a_1\mathbf{R}a_2$ and $a_2\mathbf{R}a_1\Rightarrow a_1=a_2\ \forall\ a_1,a_2\in A$

Equivalence relation

If **R** happens to satisfy properties (i), (ii) and (iii), we further say that **R** is an **equivalence relation** on **A**. Since certain structures developed during the project rely on the concept of equivalence relations, it pay to gain some insights as to what an equivalence relation really is.

Suppose you have a group of 10 people and your job is to split them up into certain smaller groups. Everybody must belong to some groups and we also do not allow people to belong to more than one group. Of course, if you are lazy, you can just arbitrarily split them anyhow you please. But your splitting would most probably be meaningless and if you encounter the same 10 people 20 years later, chances are you will not be able to remember how you once partitioned them. Alternatively, you could try to define an equivalence relation on them. Tell them that a will go to the same group as b if and only if a is related to b. Then you will be able to remember their groups if you just remember the equivalence relation that you assigned. And you will not even need to split them manually. Just tell them the rule of the relation and they can split themselves up. We now probe why the 3 properties are essential in order for us to achieve this effect.

(i) Reflexive

Suppose that, under your relation, Gary is not related to himself. He hunts around and meets Peter. On further inquiry, he discovered that he is related to Peter. Happily, he declared that he belongs to Peter's group. Joshua, who does not really like Gary very much, objected. He says that Gary can never belong to any group. If he does, then since Gary is not related to himself, he has to be taken out the very instant he attempt to join any group since his mere presence in the group will alter the property of the group in such a way that he becomes unfit to belong. Hence, the relation you define must be at least reflexive to avoid such a situation. Also, this property assures us that everybody will belong to some group. Although Joshua might not be related to anybody else in the group, he can still form a group all by himself.

(ii) Symmetric

Just now, we mentioned that Gary is related to Peter. It may very well happen that Peter is not related to Gary. In this case, we end up with a similar contradiction. Hence, symmetry is also crucial. Note that with symmetry, a relation loses hierarchy. A father-son relationship is never symmetric, since hierarchy is always involved. If Ken and Kenny are father and son, we need to specify further who is the father. In a symmetric relation, we can simply say that Ken and Kenny are related. In this sense, related elements are somehow viewed as equal in the relation.

(iii) Transitive

This is the last safeguard against exactly the same contradiction mentioned above. Also, it prevents a person from belonging to 2 different groups. Let us say that 9 people have managed to split into 3 groups and all are waiting for Gary to choose his group. Under the relation, is he going to join one of the 3 groups or form a group of his own? Suppose he discover that he actually belong to 2 of the existing 3 groups! Can this be possible? By transitivity (and symmetry), every member of one group would be related to all members of the other group through Gary. Then there should be only one group instead of 2! Hence, we see that no person can belong to 2 different groups under an equivalence relation.

We see that an equivalence relation on any non-empty set is really nothing more than a partition of the set. The groups that we informally mentioned above are actually called **equivalence classes**. We usually denote a particular equivalence class by the name of any element in the class encased in brackets. For example, if a certain equivalence class contain only Gary, Peter and Joshua, we can refer to this equivalence class as [Gary], [Peter] or [Joshua]. It does not matter which, since any element of an equivalence class would have uniquely determined the nature of the class. Let **R** be an equivalence relation on A. Formally, we define the equivalence class of any element, a, in A by

$[\mathbf{a}]=\{ b\in A \mid a\mathbf{R}b\}$

We can always form a new set **A/R** by

$\mathbf{A/R}=\{[a] \mid a\in A\}$

This set is just the set of all equivalence classes of **R** on A and as such would tend to have lesser elements than A. Beware of confusing a with [a]. [a] can be equal to [b] even though $a\neq b$. Here, what a and b actually is are irrelevant to us. They may have quite different properties but as long as they share all the properties demanded by **R**, it is enough for us to say [a]=[b]. Some results on equivalence relation can be found in the general proof section. Basically, they are just rigorous proofs of what we have already intuitively stated.

Partial order

We say that **R** is a **partial order** on A if **R** possess properties (i), (iii) and (iv). A partial order is like a queuing machinery. Imagine the same 10 person mentioned above are to be placed on a straight line. We can interpret a**R**b as meaning that a is to be placed before or together with b. As with equivalent relation, we briefly discuss the 3 properties that makes this possible.

(i) reflexive

This forces everybody to participate in the ordering, since everyone would by necessity be affected by **R**.

(iii) transitive

Of course, if we imagine the 10 person to be queuing up, then if Gary is in front of Joshua and Joshua precedes Peter, it is certainly clear that Gary will be before Peter also.

(iv) Anti-symmetry

In a sense, this is the essence of a partial order. Simply put, it does not allow 2 *different* person to be in front and behind each other at the same time, giving the basic structure of a queue.

We usually denote a partial order on A by(A, ≥). Note that in a partial order, it is possible for 2 distinct elements to share the same 'position'. If we want to avoid such a situation, we can further stipulate that **R** must also satisfy

(v) Totality

$\forall$ a, b$\in$A, either a**R**b or b**R**a

In this case, we call **R** a **total order**. Now, the crucial reason why it is possible for 2 distinct elements to be 'positioned together' by a partial order is that they can avoid being related. When the order becomes total, (v) would render this impossible.

Infimum and Supremum

Let (A, ≥) be a partially ordered set and let B be any non-empty subset of A. An element x$\in$A is called an **upper bound** of B if $x \geq y\ \forall\ y\in B$. Similarly, an element z$\in$A is called a **lower bound** of B if $y \geq z\ \forall\ y\in B$. Let U(B) and L(B) denote the set of upper and lower bounds of B respectively. We say that x is a **Supremum** of B, written as SupB, if x$\in$U(B) and $y \geq x\ \forall\ y\in U(B)$. Similarly, z is called an **Infimum** of B, written as InfB, if z$\in$L(B) and $z \geq y\ \forall\ y\in L(B)$. We will prove in the general proof section that InfB and SupB, if they exist, are unique.

An element x$\in$B is called a **Maximum** of B, written MaxB, if $x \geq y\ \forall\ y\in B$. Similarly, an element z$\in$B is called a **Minimum** of B, written MinB, if $y \geq z\ \forall\ y\in B$. It should be quite obvious that MaxB (MinB) if it exists will also necessarily be SupB (InfB). Hence, the maximum and minimum of B must also be unique if they exist.

Well-ordered set

A partially ordered set (A, ≥) is said to be **well-ordered** if for every non-empty subset B of A, MinB exists. We will elaborate more on well-ordered sets in Chapter 1, when we show that the natural number system is actually an well-ordered set.

Order Completeness

Let (A, ≥) be a partially ordered set. We say (A, ≥) has the **least upper bound property** if for every non-empty subset B of A, SupB exists whenever B is bounded above. Similarly, we say (A, ≥) has the **greatest lower bound property** if for every non-empty subset B of A, InfB exists whenever B is bounded below. If (A, ≥) has both the least upper bound property and the greatest lower bound property, then we say that (A, ≥) is **order complete**. We will defer discussion of order completeness to chapter 4, where it figures as a major theme.

Function

This is a much-used concept throughout this project. A **function** is just a special relation with the restriction that every element in its domain has one and only one image. Formally, we say that **F** is a function from A to B if

(i) **F** is a relation from A to B

(ii) Whenever $(a,b_1),(a,b_2)\in \mathbf{F}$, then $b_1=b_2$.

Although a function is, strictly speaking, a form of relation, we do not usually use the usual relation notation a**F**b. Instead, it is more intuitive to use the familiar notation F(a)=b, i.e F(a)=b iff a**F**b. Notice that this notation is more restrictive, since it implicitly allows us to attach only one element to F(a). But this is in fact the essence of a function, i.e, an element can have only one image!

A function is called **one-one** if no two elements in **D**(**F**) share the same image. In other words, if $(a_1,b),(a_2,b)\in \mathbf{F}$, then $a_1=a_2$. Furthermore, we say **F** is **onto** B if **R**(**F**) is the whole of B. That is to say, given any $b\in B$, there exist $a\in$ **D**(**F**) such that

$(a,b)\in \mathbf{F}$. We also call **F** **bijective** if it is both one-one and onto. The identity function, $\mathbf{I_A}$, from A onto A is defined by

$(a,a)\in \mathbf{I_A}$ for all $a\in A$.

That is, the identity function simply maps any element back to itself. This of course means that the identity function must always have the same domain and range. Also, whenever we write **F**:A→B, it is clear that we mean the domain of **F** to be the whole of A but the range of **F** need not necessarily be the whole of B.

We can also form composition of functions. If **F**: A→B and **G**:B→C are functions, then we say that the composite of **F** with **G** is given by

$\mathbf{G}\circ\mathbf{F}=\{(a, c)\in A\times C \mid \exists\ b\in B \text{ such that } (a, b)\in \mathbf{F}, (b, c)\in \mathbf{G}\}$

Basically, **G∘F** means taking an element, a, in the domain of **F**, calculate its image under **F**, and then passes the image **F**(a) into **G** to get the final result. This process is always well defined since we have stipulated implicitly that the range of **F** is always a subset of the domain of **G**. Also, **G∘F** remains a function itself, as proved in the general proof section.

Infinity

A nonempty set, A, is said to be infinite if there exists a proper subset B of A and a bijective function F:A→B. If a set is empty or is not infinite, then we say it is finite.

By negating the definition, we can directly say that a set A is finite if it is empty or every one-one function F:A→A is also onto. Although both definitions are equivalent, the second statement would tend to sound more intuitively obvious than the first. If we are going to put 10 balls into 10 holes with no two balls sharing the same hole, then it should be quite obvious that all 10 holes would always be filled. But if we have infinite balls and infinite holes, then it is not so clear that it is possible to find a way to leave some holes out, especially when we implicitly assumed that the numbers of holes and balls, though infinite, are ‘equal’. Yet if we accept the former case as intuitively obvious, then the latter should follow as a logical consequence. Hence, infinity may not sound so strange or counterintuitive if we just take it as meaning *having properties that differ from finiteness*.

Binary operation

Let A be a nonempty set. A function ϕ: $A\times A\to A$ is called a **binary operation** on A.

Throughout the course of this project, we will encounter quite a number of binary operations. We will clarify here what it means for a binary operation to be well defined. Usually, we will define a particular binary operation by giving a rule on how to operate on two arbitrary elements of A to produce another element, also in A. In most cases, the context of the rule itself would already implicitly show that $D(\phi)=A\times A$ and that ϕ is closed, i.e. $R(\phi)\subseteq A$. Hence, in our proofs, we do not normally mention this explicitly. What will not be immediately obvious is the requirement that no element in $A\times A$ can have 2 distinct image under ϕ. Hence, the main thrust of most proofs for the existence of well-defined binary operation would be checking this property. In the early stage, some binary operations are built directly from existing functions, and so the proof would naturally run differently.

We further define here some concepts associated with binary operations.

(i) ϕ is **associative** if

$\phi(\phi(x, y), z)= \phi(x, \phi(y, z))\ \forall\ x, y, z\in A$

(ii) ϕ is **commutative** if

$\phi(x, y)= \phi(y, x)\ \forall\ x, y\in A$

(iii) An element $e\in A$ is said to be an **identity element** for ϕ if

$\phi(x, e)= x= \phi(e, x)\ \forall\ x\in A$

(iv) We suppose an identity element, e, exist for ϕ. An element $x^{-1}\in A$ is said to be a **ϕ-inverse** of $x\in A$ with respect to e if

$\phi(x, x^{-1})= e= \phi(x^{-1}, x)$

(iv) Let ϕ, ψ be 2 binary operation on A.

We say ψ is **right distributive** over ϕ if

$\psi(\phi(x, y), z) = \phi(\psi(x, z), \psi(y, z))\ \forall\ x, y, z\in A$

Similarly, ψ is **left-distributive** over ϕ if

$\psi(z, \phi(x, y)) = \phi(\psi(z, x), \psi(z, y))\ \forall\ x, y, z\in A$

Some common properties regarding these concepts are proved in the general proof section. Observe that the notation used is very cumbersome. Usually, we will just represent a binary operation with a symbol, say *, and we write $\phi(x, y)= x*y$. This notation is more familiar and intuitive, and if we rewrite the above properties with this notation, they will look less horrendous. Also, note that when we write $x_1*x_2*...*x_n$, what we really mean is $\phi(...\phi(\phi(x_1, x_2), x_3)... ,x_n)$. Finally, whenever there is no ambiguity, x*y will be simply written as xy.

Groups and semi-groups

A **semi-group** is a non-empty set G with a binary operation * defined on it which is associative. We denote it by (G, *).

A semi-group (G, *) is called a **group** if it further satisfies the following properties:

(i) An identity element, e, exist for (G, *).

(ii) For every $x\in G$, x^{-1} exist with respect to e.

Note that in a group (or semi-group), the binary operation itself is of paramount importance. The same set, G, can become a totally different group if we give it a different binary operation. In fact, the nature of the binary operation defined totally determines the nature of the group. We will say more on this when we encounter the concept of isomorphism.

A subset, G', of G is called a sub semi-group (group) of (G, *) if (G', *) is itself also a semi-group (group). We will prove some results in the general proof section that tells us that we need not go through all the properties when checking for sub semi-group (group).

Isomorphism

Whenever we say that two structures are isomorphic, we mean that the two structures are really the same except possibly for a difference in labeling. This may sound rather abstract and informal now but we assure the reader that everything would become clearer at the beginning of our construction, where isomorphism (between natural number system) would be portrayed in more detail and depth. Some readers might be expecting a rigid definition for isomorphism but we are unable to provide it here, for technical reasons. We must understand that structures (mathematical or otherwise) come in various shapes and sizes. In order to define isomorphism for a particular type of structure, we need to know the nature of the structure (whether it be a group, ring, etc.) and suit our definition to the machinery of the structure. Hence, no general definition of isomorphism can exist that works for all forms of structures. Nevertheless, we note that there are properties of isomorphism that we would intuitively expect to be true, whatever its technical definition might be. For example, since isomorphism expresses the idea of similarity between structures, we would expect it to be an equivalent relation. Of course, we will have to prove this every time we define isomorphism for a new type of structure. It is no good to simply say that this is intuitively obvious for an isomorphism. But having all these 'expected' properties for an isomorphism at the back of our mind helps, since if we are unable to prove any one of them for a particular isomorphism, then perhaps our definition does not really hold up and we should revise it. Although the discussion on isomorphism for natural system deals specifically with only one type of structure, it is comprehensive and general enough to apply to most cases. Therefore, we shall henceforth give only technical details for whatever isomorphism we need define and refrain from repetitive explanations.

Isomorphism (for semi-groups)

We say that a semi-group $(G, *)$ is isomorphic to a semi-group $(G', *')$ if $\exists$ a bijective function $\phi: G \to G'$ such that
$\phi(x*y) = \phi(x)*'\phi(y)\ \forall\ x, y \in G$.
ϕ is called an isomorphism from $(G, *)$ to $(G', *')$.

We write $(G, *) \simeq (G', *')$ if $(G, *)$ is isomorphic to $(G', *')$. Since a group is also naturally a semi-group, this definition for isomorphism apply to groups as well.

Ring

Let R be a set with 2 binary operations on it, denoted by + and .. We say that (R, +, .) is a **ring** if
(i) (R, +) is a commutative group
(ii) (R, .) is a semi-group
(iii) . is distributive over +.

Unlike a group, a ring has 2 binary operations defined on it. It is the interaction of these two binary operations as demanded by (iii) that distinguish the properties of a ring from a group. Note that all properties of + and . on R are similar to that of a group(or semi-group) when applied in isolation. Hence, we will have a lot of properties being inherited from group structure. When we look at ring, we are mainly concerned with properties when both + and . are involved, and it is mostly such properties that require detailed proofs. We usually denote the +-inverse of x by –x and the .-inverse of x(whenever it exists) by x^{-1}. Also, it is usual to write x+(-y) as x-y and x.y as xy. When we deal with specific structure(for example, $\mathbb{Q}$ is actually a field), we will usually use this familiar shorthand notation. We list here some special types of ring that will prove to be important in our construction.

(a) (R, +, .) is called a **commutative ring** if (R, .) is a commutative semi-group.

(b) (R, +, .) is a **ring with unit** if $\exists$ $1\in R$, $1 \neq 0$ s.t 1 is the identity element for (R, .).

(c) Let (R, +, .) be a commutative ring with unit.

If a.b = 0 $\Rightarrow$ a = 0 or b = 0 $\forall$ a, $b\in R$, then we say that (R, +, .) is an **integral domain**.

(d) Let (R, +, .) be an integral domain.

If $\forall$ $a\in R\backslash\{0\}$, a^{-1} exist, then we say that (R, +, .) is a **field**.

Proving the properties of rings, integral domains and fields will turn out to be useful in our construction since they appear quite often as a specific structure. Note that a lot of properties(though worthy to be mentioned) are direct consequence of the definition or inherited from previous structures. Hence, such obvious properties will be listed without much comment.

As with the case for groups, we say that a subset R' of R is a sub ring (integral domain, field) of (R, +, .) if (R', +, .) is itself also a ring (integral domain, field). The definition for integral domain, field etc may not always be the most practical definition to use and so we will show in the general proof section other equivalent definitions so that the identification of such structures need not involve so much work. Furthermore, it is usually not essential to check through all the properties for sub structures and so such alternative definitions can usually help provide essential criteria for a subset to qualify as a sub structure.

Mainly for ease of development when we encounter sequences, we will proclaim here that the familiar notation for natural number will be employed generally in a field as follows. As said earlier, 1 is used for the multiplicative identity. We denote 1+1 as 2, (1+1)+1 as 3 and so on. When we write x/y, we mean $x.y^{-1}$. Hence, whenever we claim that $\varepsilon > \varepsilon/2$ for $\varepsilon > 0$ in an ordered field, the reasoning behind it is the following. We have 2=1+1>1>0. This means $0< 2^{-1}<1$. As $\varepsilon >0$, we then have $\varepsilon.1 > \varepsilon.2^{-1}$. All these individual claims which leads to the conclusion is justified in the general proof section. What is important to remember here is this. We are only borrowing notation, and a field is defined independently of the natural numbers. Nonetheless, intuitive order relation for real number are usually still valid in an ordered field, and the sharing of this notation simplify things greatly. The reader should be aware that nothing has been assumed. Even though we casually claim that $\varepsilon > \varepsilon/2$ in most proofs, it is not a result through our intuitive 'number sense'. Rather, it is a simple consequence of the properties of ordered integral domain proven in the general proof section, after we have clarified the meaning of the notation 2. Finally, we sometimes also write something like ε^4. This is not to be taken as a definition for exponentiation in an ordered field. It should just be viewed as a shorthand for writing ε.ε.ε.ε.

Isomorphism (for rings)

We say that a ring (R,+, .) is isomorphic to a ring (R', $+'$,$.'$) if $\exists$ a bijective function ϕ: R$\rightarrow$ R' such that $\forall$ x, $y\in R$,

(i) $\phi(x+y) = \phi(x)+'\phi(y)$

(ii) $\phi(x.y) = \phi(x).'\phi(y)$

ϕ is called an isomorphism from $(R, +,.)$ to $(R', +',.')$. We write $(R, +,.) \simeq (R', +',.')$ if $(R, +,.)$ is isomorphic to $(R', +',.')$. Naturally, this definition also apply to special types of rings such as integral domain, field etc.

Ordered integral domain

Let $(R, +, .)$ be any integral domain. Suppose there exist a subset P of R such that

a) $\forall x, y \in P, x+y, x.y \in P$

b) $\forall x \in R$, one and only one of the following holds: $x \in P, x=0, -x \in P$

Define the relation $>$ by $x>y$ iff $x-y\in P$. We then say that $(R,+,.,>)$ is an ordered integral domain. Observe that $x>0$ iff $x=x-0\in P$ so instead of saying $x\in P$, it is usual and equivalent to write $x>0$ for algebraic manipulation.

For an ordered integral domain $(R,+,.,>)$, we can define a new relation $\geq$ by $\forall x, y \in R, x \geq y$ iff $x>y$ or $x=y$. These two relations will be the most frequently used when we try to order our number system.

Isomorphism (for ordered integral domain)

We say that an ordered integral domain $(R,+, .,>)$ is isomorphic to an ordered integral domain $(R', +',.',>')$ if $\exists$ a bijective function $\phi: R\rightarrow R'$ such that $\forall$ x, $y\in R$,

(i) $\phi(x+y) = \phi(x)+'\phi(y)$

(ii) $\phi(x.y) = \phi(x).'\phi(y)$

(iii) $x>y \Rightarrow \phi(x)>'\phi(y)$

ϕ is called an isomorphism from $(R, +,.,>)$ to $(R', +',.',>')$. We write $(R, +,.,>) \simeq (R', +',.',>')$ if $(R, +,.,>)$ is isomorphic to $(R', +',.',>')$. Naturally, this definition also apply to special types of ordered integral domain such as ordered field.

Absolute Value

Let $(F, + ,. ,>)$ be an ordered field. For any $x\in F$, we define the absolute value of x by

$|x|= x$ if $x \geq 0$
$-x$ if $x < 0$

The concept of absolute value is essential for us to make sense of the notion of the limit of a sequence in an ordered field. Some intuitive and useful properties of absolute value will be developed in the general proof section.

Sequences

Let $(F, +, . ,>)$ be an ordered field. We assume here the existence of $\mathbb{N}$, the set of natural number, together with its properties. Since sequences will only be invoked from the rationals onwards, this assumption is valid. We can define a sequence to be a function $f: \mathbb{N} \rightarrow F$ s.t

$f(n) = x_n$

and we denote this by (x_n). The element x_n is called the n^{th}- term of the sequence.

Intuitively, a sequence is just an ordered collection of elements in F. Our definition is just a sophisticated way of representing a queue like this:

1	2	3	4	5	6...	n...
x_1	x_2	x_3	x_4	x_5	x_6...	x_n...

We can also form subsequences from sequences. Formally, we say that (y_n) is a subsequence of (x_n) if for each $n \in \mathbb{N}$, we have

$y_n = x_k$ for some $k \in \mathbb{N}$ and

$y_{n+1} = x_i$ for some $i \in \mathbb{N}$ and $i > k$

Intuitively, we can just imagine a subsequence of a sequence as a sequence that is formed by skipping terms of the original sequence. For example, we can say that

$x_2, x_5, x_7, 1, 1, 1, \ldots$

is a subsequence of

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, 1, 1, 1\ldots$

A lot of important results associated with sequences relate to their subsequences also. Some are easy, but technical notation usually makes the proof longer than necessary. In such cases, the author feels that the reader will be better off relying on his intuition rather than unraveling the technicalities of the proof to 'see' the result. A special type of subsequence, called the k-tail of the sequence (x_n) is defined by

$y_n = x_{n+k-1} \ \forall \ n \in \mathbb{N}$.

Hence, a sequence is always the 1-tail of itself. In most application of sequences, we are mainly concerned with the "eventual behavior" of the sequence and hence in this respect, it should be intuitively clear that any tail of the sequence behaves the same as the original one.

A sequence is increasing if $x_{n+1} \geq x_n \ \forall \ n \in \mathbb{N}$. Similarly, a sequence is decreasing if $x_{n+1} \leq x_n \ \forall \ n \in \mathbb{N}$. A monotone sequence is one that is either increasing or decreasing.

We will now mention some major concepts associated with sequences.

Limit (convergent sequences)

We say that (x_n) has a limit $x \in F$ if given any $\varepsilon > 0$, $\varepsilon \in F$, $\exists \ k \in \mathbb{N}$ s.t

$| x_n - x | < \varepsilon \ \forall \ n \geq k$

If (x_n) has a limit x, then we write

$\lim x_n = x$ or simply $(x_n) \rightarrow x$.

Intuitively, if $(x_n) \rightarrow x$, then the terms are "getting closer" to the element x with respect to the order defined. If they are getting closer to a particular x, then it seems that they must also be getting closer to one another. This intuition is correct, and we will later make it more precise when we define Cauchy sequences. For now, we note that a sequence can have at most one limit (proven in the general proof section but should be intuitively clear) so we can hence unambiguously say that (x_n) converges to x. We say that (x_n) is convergent if its limit exists.

Cauchy sequences

We say that (x_n) is a Cauchy sequence if given any $\varepsilon > 0$, $\varepsilon \in F$, $\exists \ k \in \mathbb{N}$ s.t

$| x_n - x_m | < \varepsilon \ \forall \ n, m \geq k$.

This is the precise formulation of a sequence having its terms eventually clustering around one another. We mentioned earlier that every convergent sequence is necessary Cauchy. Is the converse also true? Well, it is not and this seems to go against our intuition. Why should terms not cluster around some particular element if they are clustering around themselves? To work this out, the author feels that it would be illuminating to focus on the asymmetry of the situation. We will use an example that closely parallel the real number system.

Imagine that the whole human race is being tightly queued up on a very long line. By some strange method of human measurement, suppose that there is a sequence of males that converges to Gary. This translate roughly to mean that no matter how tiny the “distance” one demands, eventually all the males from some k^{th} male onward in the sequence will be at most that far from Gary. Hence, those males should be at most twice that distance(since the males can be to the left or right of Gary) from one another. There seems to be no problem concluding then that they are Cauchy. But suppose this sequence of males is only Cauchy. Would they not cluster around some human? The author would not be arguing against that. In fact, his intuition totally agrees with that. There is no reason why one should accept that clustering around one particular person naturally means clustering together but reject the converse implication. The crux of the matter has more to do with the sex of this important person! Are we assured that this person is a male? If this person is a female, then she rightly does not belong to the male domain and hence the condition that the limit element must belong to the field is not satisfied. Hence, a Cauchy sequence need not always be convergent, due to perhaps “holes” in the field. Of course, this example is not really “accurate” or “mathematically precise”. The definition require that we use elements in the field to measure distance and we have not really indicate how to measure with humans. Nonetheless, it should have served its purpose as an intuitive argument.

If it happens that every Cauchy sequence is also convergent, then we say that F is Cauchy complete.

End Of Definition Section

GENERAL PROOF SECTION

This section contains basic proofs of diverse concepts in mathematics. Most of these results have been simply assumed in the construction process since to prove or mention them explicitly there would obstruct the flow of the construction. Also, most of such results are intuitively obvious and a formal proof really is truly only for the sake of formality. On the other hand, there are results (such as those regarding sequences or the algebra of integral domain) that are quite central to our theme. But such results are usually global in nature(for example, the integer system, field of rationals and the real number system can all share the same basic algebra of integral domain) so they are placed here to enable common access and hence avoid repetitive proofs. As a general rule, a mature reader can simply skimp through this section but he should be aware that any algebraic manipulation used during the construction has indeed been justified in this section. It would be fun to view these results as our basic mathematical toolkit provided for the construction.

Theorem:

Let R be an equivalence relation on a set X. Then the following holds:
(i) [a]=[b] iff aRb
(ii) $[a]\cap[b]=\varnothing$ iff $(a, b)\notin R$
(iii) $X=\{b \mid b\in[a]$ for some $a\in X\}$

(i) Suppose that [a]=[b]. By reflexivity, we have bRb so $b\in[b]=[a]$, i.e aRb. Now suppose that aRb. Take any $c\in[b]$. We have bRc and so by transitivity, we have aRc and so $c\in[a]$. Hence, $[b]\subseteq[a]$. Since by symmetry we also have bRa, this must mean that $[a]\subseteq[b]$ also. Hence, [a]=[b].

(ii) Suppose that $[a]\cap[b]=\varnothing$. If aRb, then by (i), [a]=[b] so that we must have

$[a]= [a]\cap[b]=\varnothing$. But reflexivity tells us that aRa, i.e $a\in[a]$ which is a contradiction.

Now suppose $(a, b)\notin R$. If $c\in[a]\cap[b]$, then we have aRc and bRc. By symmetry, we have cRb and so by transitivity, aRb, a contradiction! Hence, $[a]\cap[b]=\varnothing$.

(iii) For any $x\in X$, we have xRx so that $x\in[x]$ and hence $x\in\{b \mid b\in[a]$ for some $a\in X\}$. For any $b\in\{b \mid b\in[a]$ for some $a\in X\}$, we have $b\in[a]$ for some $a\in X$ and since [a] is a subset of X by definition, we will have $b\in X$ also. Hence, $X=\{b \mid b\in[a]$ for some $a\in X\}$

Q.E.D

Theorem:

Let $F: A \to B$ be a bijective function. Then the inverse of F, which we define by
$F^{-1} = \{(b, a)\in B\times A \mid (a, b)\in F\}$
is also a bijective function with $D(F^{-1}) = B$

Suppose F^{-1} is not a function. Then $\exists$ $(b, a_1), (b, a_2)\in F^{-1}$ s.t $a_1 \neq a_2$.

This contradicts the one-one nature of F. Also, if $D(F^{-1})\neq B$, then $\exists$ $b\in B$ s.t $(b, a)\notin F^{-1}$ $\forall$ $a\in A$. This contradict the onto nature of F. Hence we can say $F^{-1}: B \to A$ is a function.

Suppose F^{-1} is not one-one. Then $\exists$ (b_1, a), $(b_2, a)\in F^{-1}$ s.t $b_1 \neq b_2$. This contradicts the fact that F is a function.

Suppose F^{-1} is not onto. Then $\exists$ $a\in A$ s.t $(b, a)\notin F^{-1}$ $\forall$ $b\in B$. But $D(F) = A$, hence this is not possible.

Therefore, $F^{-1}: B \to A$ is also a bijective function.

Q.E.D

Theorem:

Let $F: A\to B$ and $G: B\to C$ be functions. Then the composite of F with G, which we define by

$G\circ F= \{(a, c)\in A\times C \mid \exists\, b\in B$ s.t $(a, b)\in F, (b, c)\in G\}$

is also a function with $D(G\circ F) = A$.

If $G\circ F$ is not a function, then $\exists$ (a, c_1), $(a, c_2)\in G\circ F$ s.t $c_1 \neq c_2$. Hence, $\exists$ $b_1, b_2\in B$ s.t (a, b_1), $(a, b_2)\in F$, (b_1, c_1), $(b_2, c_2)\in G$. Since F is a function, it follows that $b_1= b_2$. We then have a contradiction since this would mean that G is not a function. Now take any $a\in A$. Since $D(F) = A$, $\exists$ $b\in B$ s.t $(a, b)\in F$. As $D(G) = B$, we also have $(b, c)\in G$ for some $c\in C$. Hence, $(a, c)\in G\circ F$. Hence $D(G\circ F) = A$.

Therefore, $G\circ F: A\to C$ is also a function.

Q.E.D

Theorem:

Let A, B be non-empty sets and $F: A\to B$ be a bijective function.
Then $F^{-1}\circ F = I_A$ and $F\circ F^{-1} = I_B$.

Take any $(a_1, a_2)\in F^{-1}\circ F$. By the definition of composition, $\exists$ $b\in B$ s.t $(a_1, b)\in F$, $(b, a_2)\in F^{-1}$. By the definition of inverse, we must have $(b, a_1) \in F^{-1}$. Since $F^{-1}: B\to A$ is a function, it follows that $a_1 = a_2$. Hence, $F^{-1}\circ F = I_A$. By symmetry, we hence also have $F\circ F^{-1} = I_B$.

Q.E.D

Theorem:

Suppose $F: A\to B$, $G: B\to A$ are functions and that $G\circ F = I_A$, $F\circ G = I_B$. Then both F and G are bijective.

We first show that F is bijective. Then G is bijective follows simply by symmetry.

Take any (a_1, b), $(a_2, b)\in F$. Now, $\exists$ an unique $a_3\in A$ s.t $(b, a_3)\in G$. Hence (a_1, a_3), $(a_2, a_3)\in G\circ F$. But $G\circ F = I_A$, hence $a_1 = a_3 = a_2$ and so F is one-one.

Take any $b\in B$. Then $(b, b)\in F\circ G$ and so $\exists$ $a\in A$ s.t $(b, a)\in G$, $(a, b)\in F$. Hence, $\forall$ $b\in B$, $\exists$ $a\in A$ s.t $(a, b)\in F$ and so F is onto B.

Hence, F (and also G) is bijective.

Q.E.D

Theorem:

Let $F:A\to B$, $G:B\to C$ be functions. Then the following holds:

(i) If F,G are one-one, then $G\circ F$ is also one-one

(ii) If F,G are onto, then $G\circ F$ is also onto

Hence, If F,G are bijective, then $G\circ F$ is also bijective.

(i) Take any (a_1,c), $(a_2,c)\in G\circ F$. By the definition of composition, $\exists$ b_1, $b_2\in B$ s.t (a_1,b_1), $(a_2,b_2)\in F$, (b_1,c), $(b_2,c)\in G$. Since G is one-one, $b_1 = b_2$. Hence, since F is one-one, we must have $a_1 = a_2$. Hence, $G\circ F$ is one-one.
(ii) Take any $c\in C$. Since G is onto C, $\exists$ $b\in B$ s.t $(b, c)\in G$. Since F is onto B, $\exists$ $a\in A$ s.t $(a, b)\in F$. By definition of composition, this means $(a, c) \in G\circ F$ and so $G\circ F$ is onto C.
Q.E.D

Theorem:
Let $A \subseteq B$. Then B is infinite if A is infinite.

Since $A \subseteq B$, we can always write $B = A\cup E$ where $A\cap E = \phi$ for some set E.
Since A is infinite, $\exists$ a one-one function $f: A\rightarrow A$ which is onto some proper subset A' of A. Define $f': B\rightarrow B$ by

$f'(x) = f(x)$ if $x\in A$
$\qquad x \quad$ if $x\in E$

Then f' is one-one since f is one-one, the identity function is one-one and $A\cap E = \phi$.
Also, $R(f') = A'\cup E$ which is a proper subset of B. Hence, A is also infinite.
Also, A is finite if B is finite follow by contra-postivity.
Q.E.D

Theorem:
Let A and B be any 2 sets. Suppose there exists a bijective function $f: A\rightarrow B$. Then A is infinite iff B is infinite.

Suppose B is infinite. Then $\exists$ a bijective $g: B\rightarrow B'$ where B' is some proper subset of B. In particular, $\exists$ $b_0\in B$ s.t $b_0\notin B'$. As f is bijective, $f^{-1}: B\rightarrow A$ is well defined and bijective. Consider the composite $f^{-1}\circ g\circ f: A\rightarrow A$. $f^{-1}\circ g\circ f$ is one-one since it is the composite of one-one functions. Consider the element $a_0= f^{-1}(b_0) \in A$. Since f^{-1} is one-one, $f^{-1}(b) \neq a_0$ $\forall$ $b \neq b_0$. For every $a\in A$, $g\circ f(a) \neq b_0$ since g is onto B', i.e $f^{-1}\circ g\circ f(a) \neq a_0$. Hence, $f^{-1}\circ g\circ f$ is onto some proper subset A' of A. In other words, $f^{-1}\circ g\circ f: A\rightarrow A'$ is a bijective function.
Hence, A is infinite also.
The double implication follows by symmetry since we can always consider the bijective $f^{-1}: B\rightarrow A$.
Q.E.D

Theorem:
Let $(A, \geq)$ be a partially ordered set and T a non-empty subset of A. Then
(i) If SupT exists, then it is unique.
(ii) If InfT exists, then it is unique.
(iii) If MaxT exists, then SupT=MaxT
(iv) If MinT exists, then InfT=MinT

(i) Let x_1, $x_2\in A$ be 2 suprema for T. Then since x_1 is a suprema and x_2 an upper bound, we have $x_2 \geq x_1$. Similarly, $x_1\geq x_2$. Hence $x_1 = x_2$ by anti-symmetry and so SupT is unique whenever it exists.
(ii) Let x_1, $x_2\in A$ be 2 infimum for T. Then since x_1 is an infimum and x_2 a lower bound, we have $x_1 \geq x_2$. Similarly, $x_2 \geq x_1$. Hence $x_1 = x_2$ by anti-symmetry and so InfT is unique whenever it exists.

(iii) Obviously, MaxT is an upper bound of T. Since MaxT$\in$T, x $\geq$ MaxT if x is an upper bound of T. Hence, SupT=MaxT.

(iv) Obviously, MinT is a lower bound of T. Since MinT$\in$T, MinT $\geq$ x if x is a lower bound of T. Hence, InfT=MinT.

Q.E.D

Theorem:

Let (G, *) be a group. Then $\forall x, y, z \in G$, the following holds:

(i) The cancellation law holds

$xy= xz \Rightarrow x^{-1}(xy)=x^{-1}(xz)$

$\Rightarrow (x^{-1}x)y=(x^{-1}x)z$ (associativity)

$\Rightarrow ey=ez$

$\Rightarrow y=z$

Similarly, $yx= zx \Rightarrow y=z$

Hence, the cancellation law holds.

(ii) The identity element, e, is unique

Let e and e′ be two identity element. Then

ee′=e (since e′ is an identity element)

ee′=e′ (since e is an identity element)

Hence, e= ee′ =e′ and so the identity element is unique.

(iii) The inverse of x is unique

Let x^{-1} and $x^{-1\prime}$ be 2 inverses for x. Then

$x^{-1}x=e= x^{-1\prime}x$

$\Rightarrow x^{-1}=x^{-1\prime}$ (by (i))

Hence, the inverse of x is unique.

(iv) The inverse of x^{-1} is x itself

By the definition of inverse, we have $xx^{-1}=e= x^{-1}x$. But this equation also show that $(x^{-1})^{-1} =x$.

(v) $e^{-1}=e$

This follows easily from the equation ee=e.

(vi) $(xy)^{-1}=y^{-1}x^{-1}$

This is by direct verification since

$(xy)(y^{-1}x^{-1})= ((xy)y^{-1})x^{-1}$ (associativity)

$= (x(yy^{-1}))x^{-1}$ (associativity)

$=(xe) x^{-1}$

$=xx^{-1}$

$=e$

Similarly, $(y^{-1}x^{-1})(xy)=e$

Hence, $(xy)^{-1}=y^{-1}x^{-1}$

In the general case, let

$P=\{n\in \mathbb{N}| (x_1x_2...x_n)^{-1}=x_n^{-1}x_{n-1}^{-1}...x_1^{-1} \ \forall\ x_1,x_2,...,x_n \in G\}$

Obviously, $1\in P$.

Suppose $n\in P$. Take any $x_1,x_2,...,x_n,x_{n+1} \in G$. Then

$(x_1x_2...x_nx_{n+1})^{-1}= x_{n+1}^{-1}(x_1x_2...x_n)^{-1}$ (by preceding result)

$=x_{n+1}^{-1}x_n^{-1}x_{n-1}^{-1}...x_1^{-1}$ (by induction hypothesis)

Hence, $S(n) \in P$ whenever $n\in P$. By N(v), $P=\mathbb{N}$ and so

$(x_1x_2...x_n)^{-1}=x_n^{-1}x_{n-1}^{-1}...x_1^{-1} \ \ \forall\ n\in \mathbb{N}$.

Q.E.D

Theorem:

Let A be a non-empty set and $*$ be a binary operation on A that is both associative and commutative. Then the following holds:

(i) Let $x_1, x_2,\ldots, x_n \in A$. Then

$x_1x_2\ldots x_n = x_{i(1)}x_{i(2)}\ldots x_{i(n)}$ where $(i_1, i_2,\ldots, i_n)$ is any permutation of $(1, 2,\ldots, n)$

Define

P = {n∈ℕ | (i) is true}.

Obviously, 1∈P. Suppose n∈P. If n = 1, then S(1)∈P by commutativity. If $n \neq 1$, then take any $x_1, x_2,\ldots, x_{n+1} \in A$. Consider also any permutation $(i_1, i_2,\ldots, i_{n+1})$ of (1, 2,…, n+1). We suppose first that $i_{n+1} \neq n+1$. Then

$x_{i(1)}x_{i(2)}\ldots x_{i(n)}x_{i(n+1)}$

$= (x_{i(1)}x_{i(2)}\ldots x_{i(n)})x_{i(n+1)}$

$= (x_{j(1)}x_{j(2)}\ldots x_{j(n-1)}x_{n+1})\, x_{i(n+1)}$ (since n∈P, we can rearrange the terms in the brackets anyhow we please. In particular, we move x_{n+1} towards the end)

$= ((x_{j(1)}x_{j(2)}\ldots x_{j(n-1)})x_{n+1})x_{i(n+1)}$

$= (x_{j(1)}x_{j(2)}\ldots x_{j(n-1)})(x_{n+1}x_{i(n+1)})$ (by associativity)

$= (x_{j(1)}x_{j(2)}\ldots x_{j(n-1)})(x_{i(n+1)}x_{n+1})$ (by commutativity)

$= (x_{j(1)}x_{j(2)}\ldots x_{j(n-1)}x_{i(n+1)})x_{n+1}$ (by associativity again)

$= (x_1x_2\ldots x_n)x_{n+1}$ (since n∈P)

$= x_1x_2\ldots x_{n+1}$

If $i_{n+1} = n + 1$, then we do not even need to shift x_{n+1} and S(n)∈P follows directly from induction hypothesis. Hence, S(n)∈P whenever n∈P and so by N(v), P = ℕ, proving our assertion.

(ii) Consider a string of expression $x_1 x_2\ldots x_n$. Obviously, there are a lot of ways to insert well-defined brackets in them. Inserting brackets is an interference in the natural order of evaluation and the final result may be affected. Note that the expression itself carry with it its own natural sets of brackets. For example,

$x_1x_2x_3x_4 = (((x_1)x_2)x_3)x_4)$

The horrendous bracketing is nothing more than saying explicitly how to carry out the operation naturally, i.e. from left to right, one term at a time. But some bracketing breaks this natural order. For example, it is not necessarily true that

$x_1x_2x_3x_4 = x_1(x_2\, x_3)x_4$

We will call such brackets forced bracketing. Our goal is to prove that all forms of forced bracketing (and hence any bracketing) gives the same result as the natural order of evaluation for (A, $*$). Let us denote this claim as (ii) for any particular n∈ℕ.

Let P = {n∈ℕ | (ii) is true for n}.

Obviously, 1∈P. Suppose {k∈ℕ | k ≤ n} ⊆ P. Consider the string $\boldsymbol{x_1x_2\ldots x_nx_{n+1}}$ undergoing some form of forced bracketing. We consider 2 cases.

(a) x_{n+1} is not within any forced brackets.

In this case, x_{n+1} is always the last input and so

$\boldsymbol{x_1x_2\ldots x_nx_{n+1}} = (\boldsymbol{x_1x_2\ldots x_n})x_{n+1}$

$= (x_1x_2\ldots x_n)x_{n+1}$ (by induction hypothesis)

$= x_1x_2\ldots x_{n+1}$

(b) x_{n+1} is within one or more forced brackets.

In this case, we consider the outer most such forced brackets. This outer most bracket must not encompass x_1, else it reduces to a natural bracket. Hence, its opening bracket start after x_1. We can then write

$\boldsymbol{x_1x_2\ldots x_nx_{n+1} = x_1\ldots x_{i-1}(x_i\ldots x_{n+1})}$

$= (\boldsymbol{x_1\ldots x_{i-1}})(\boldsymbol{x_i\ldots x_{n+1}})$ (just inserting a natural bracket)

$= (x_1\ldots x_{i-1})(x_i\ldots x_{n+1})$ (observe that the 2 brackets each contain n variables less, so that our induction hypothesis apply)

$= (x_1\ldots x_{i-1}x_i)(x_{i+1}\ldots x_{n+1})$ (associativity)

$\vdots$ (repeated application of associativity n + 1 – i times)

$= x_1x_2\ldots x_{n+1}$

Hence $S(n)\in P$ whenever $\{k\in \mathbb{N} \mid k \leq n\} \subseteq P$. By the principle of general induction, $P = \mathbb{N}$ and so our assertion holds.

Q.E.D

Now, why do we bother to prove the above result? Well, we all know that addition and multiplication on the set of real numbers (and hence its subsets) are associative and commutative. With this result, after establishing the commutativity and associativity of these two binary operations for a particular subset of $\mathbb{R}$, we can freely rearrange and insert or remove brackets in any finite strings of expression at our whim. This saves a lot of repetitive steps and allows us to focus on the 'crucial' step. Hence, in the course of our proofs, we will usually do such rearrangements silently and without comments, just as any student would have done in any other proofs. For them, the result is simply intuitively obvious, something they have been used to all this years. For us, we require justification before we can wield such powers. Since we also wish to acquire such convenient powers, we hence provide the justification!

For some readers, the idea and proof in (ii) may seem to be rather awkward and unsatisfactory. It is possible to make the idea more formal and we will demonstrate one such proof below. First, we will introduce the concept of admissible functions that are supposed to simulate all the various possible way of bracketing.

<u>Admissible Functions</u>

Let A be any non-empty set and f: AXA→A a binary operation on A. We define admissible n-extension functions, f_n: A^n→A, of f inductively as follows:

(i) There is exactly one admissible 2-extension function of f given by f itself

(ii) Suppose that f_n: A^n→A is an admissible n-extension function of f. Then f_{n+1}: A^{n+1}→A is an admissible n+1-extension function of f if there exist $1\leq m\leq n$ such that

$$f_{n+1}(x_1,\ldots,x_m,\ldots,x_{n+1}) = f_n(x_1,\ldots,x_{m-1},f(x_m,x_{m+1}),x_{m+2},\ldots,x_{n+1}) \qquad \forall (x_1,\ldots,x_{n+1})\in A^{n+1}$$

Note that in this new framework, saying that f is commutative or associative translate to mean the following:

(a) Commutativity

$f(x_1,x_2)= f(x_2,x_1) \quad \forall (x_1,x_2) \in AXA$

(b) Associativity

The admissible 3-extension function of f is unique.

The following theorem is the equivalent of (ii).

Theorem:

If f is an associative binary operation on a non-empty set A, then for every $n\in\mathbb{N}$, $n>1$, the admissible n-extension function of f is unique.

Let $P=\{n\in\mathbb{N} \mid$ the admissible n-extension function of f is unique$\}$. By definition, $2,3\in P$. Suppose $n\in P$. We may assume $n>2$ else $n+1\in P$ trivially.

Consider any arbitrary admissible n-extension function of f, f_n. We denote each possible admissible n+1-extension of f that can be created from f_n by $f_{n,m}$, $1\leq m\leq n$. We show first that for $1\leq t<n$, $f_{n,t}=f_{n,t+1}$

Now,

$f_{n,t} = f_n(x_1,\ldots,x_{t-1},f(x_t,x_{t+1}),x_{t+2},\ldots,x_{n+1})$

$f_{n,t+1} = f_n(x_1,\ldots,x_t,f(x_{t+1},x_{t+2}),x_{t+3},\ldots,x_{n+1})$

By definition, there exist an admissible n-1-extension function of f, f_{n-1}, s.t

$f_n = f_{n-1}(x_1,\ldots,x_{m-1},f(x_m,x_{m+1}),x_{m+2},\ldots,x_n)$ for some $1\leq m\leq n-1$

From this f_{n-1}, we can create an admissible n-extension function of f, $f_{n-1,t}$, by

$f_{n-1,t} = f_{n-1}(x_1,\ldots,x_{t-1},f(x_t,x_{t+1}),x_{t+2},\ldots,x_n)$

Since all admissible n-extension functions are the same by induction hypothesis, we have

$f_n =f_{n-1,t} = f_{n-1}(x_1,\ldots,x_{t-1},f(x_t,x_{t+1}),x_{t+2},\ldots,x_n)$

Hence,

$f_{n,t} = f_n(x_1,\ldots,x_{t-1},f(x_t,x_{t+1}),x_{t+2},\ldots,x_{n+1})$

$\quad = f_{n-1}(x_1,\ldots,x_{t-1},f(f(x_t,x_{t+1}),x_{t+2}),\ldots,x_{n+1})$

$f_{n,t+1} = f_n(x_1,\ldots,x_t,f(x_{t+1},x_{t+2}),x_{t+3},\ldots,x_{n+1})$

$\quad = f_{n-1}(x_1,\ldots,f(x_t,f(x_{t+1},x_{t+2})),x_{t+3},\ldots,x_{n+1})$

Since $3\in P$, we will always have $f(f(x_t,x_{t+1}),x_{t+2}) =f(x_t,f(x_{t+1},x_{t+2}))= X_t$. In other words,

$f_{n,t}= f_{n-1}(x_1,\ldots, x_{t-1},X_t,x_{t+3},\ldots,x_{n+1})= f_{n,t+1}$

As a consequence, the following equality holds:

$f_{n,1} =f_{n,2} =f_{n,3}= \ldots=f_{n,n-1} =f_{n,n}$

Hence, we have shown that the n possible admissible n+1-extension of f that can be created from any particular admissible n-extension of f are all the same. Now any admissible n+1-extension of f is created from some admissible n-extension of f by definition. We have shown that each admissible n-extension of f gives us only one unique admissible n+1-extension of f. But by induction hypothesis, the admissible n-extension of f are all the same, so this means we will only get one unique admissible n+1-extension of f! Hence, $n+1\in P$ whenever $n\in P$.

By the modified principle of induction, we then have $P=\mathbb{N}\backslash\{1\}$ and so our claim is true.

Q.E.D

Theorem:

Let (R, +, .) be an integral domain. Then the following holds:

Since (R, +) is a commutative group, we have:

(1) $\mathbf{x + y = y + x}$

(2) $\mathbf{(x + y) + z = x + (y +z)}$

(3) $\mathbf{x + 0 = x}$

(4) $\mathbf{x - x = 0}$

(5) $\mathbf{-(-x) = x}$

(6) $-0 = 0$

(7) $-(x + y) = -x - y$

$$-(x + y) = (-y) + (-x)$$
$$= (-x) + (-y) \text{ (by (1))}$$
$$= -x - y$$

(8) $x + y = x + z \Leftrightarrow y = z$

(9) $-(x - y) = y - x$

$$-(x - y) = -x - (-y) \text{ (by (7))}$$
$$= -x + y \text{ (by (5))}$$
$$= y - x \text{ (by (1))}$$

(10) $x - y = 0 \Leftrightarrow x = y$

Write $0 = y - y$ and the assertion follows from (8).

Since (R,.) is a commutative semi group, we have:

(11) $x.y = y.x$

(12) $(x.y).z = x.(y.z)$

---

(13) $1.x=x$

(14) $x.(y+z)=x.y+x.z$

(15) $x.y=0\Leftrightarrow x=0$ or $y=0$

$x.y=0\Rightarrow x=0$ or $y=0$ follows from definition of integral domain. If at least one, say y, is 0, then

$x.0=x.(0+0)$ (by (3))
$=x.0 + x.0$ (by (14))
$\Rightarrow 0=x.0$ (by (8))

(16) $-(x.y)=(-x).y$

By direct verification, we have

$x.y + (-x).y = (x + (-x)).y$ (by (14))
$=0.y$ (by (4))
$=0$ (by (15))

(17) $(-x).(-y) = x.y$

$(-x).(-y) = -(x.(-y))$ (by (16))
$=-(-(x.y))$ (by (16))
$=x.y$ (by (5))

(18) $z.(x-y)=z.x - z.y$

$z.(x-y)=z.x + z.(-y)$ (by (14))
$=z.x + (-(z.y))$ (by (16))
$=z.x -z.y$

(19) $(-1).x= -x$

From (16), we have

$-(1.x)= (-1).x$, i.e $-x = (-1).x$

Q.E.D

<u>Theorem:</u>

Let (X, +, ., >) be an ordered integer domain. Then the following hold:

(1) $x, y > 0 \Rightarrow x + y, x.y > 0$

(2) $\forall$ x, y$\in$X, exactly one of the following is true: $x > y$, $x = y$, $x < y$.

Equivalently, we need to show exactly one of the following is true: $x - y > 0$,

$x - y = 0$, $-(x - y) = y - x > 0$. But this follows from the definition. (Note that in most of the following properties, this result will be implicitly assumed.)

(3) $x > x$ is never true.

By definition, we cannot have $0 > 0$. Since $x > x \Rightarrow 0 = x - x > 0$, $x > x$ is never true.

(4) $x > y$ and $y > z \Rightarrow x > z$.

Hence, $(x - y), (y - z) > 0$. By (1), $x - z = (x - y) + (y - z) > 0$ so $x > z$.

(5) $x > y \Leftrightarrow x + z > y + z$

$x > y \Rightarrow (x - y) > 0 \Rightarrow (x + z) - (y + z) > 0 \Rightarrow x + z > y + z$. Now, by adding $-z$ to both sides, we also have the reverse implication.

(6) $x > 0 \Rightarrow -x < 0$. Similarly $x < 0 \Rightarrow -x > 0$.

By (5), $x > 0 \Rightarrow 0 = x - x > -x$. Similarly, $x < 0 \Rightarrow 0 = x - x < -x$.

(7) For $x \neq 0$, $x.x > 0$

If $x > 0$, then this follows from (1). If $x < 0$, then $-x > 0$ by (6). Hence, $x.x = (-x).(-x) > 0$ by (1).

(8) $-1 < 0 < 1$

Now, $1 = 1.1 > 0$ by (7) since $1 \neq 0$. Together with (6), we have $-1 < 0 < 1$.

(9) $x, y < 0 \Rightarrow x + y < 0, x.y > 0$

By (6), $-x, -y > 0$. Then $-(x + y) = -x - y > 0$ by (1). By (6), this means $x + y < 0$. Also, $x.y = (-x).(-y) > 0$ by (1).

(10) $x.y > 0 \Leftrightarrow (x > 0$ and $y > 0)$ or $(x < 0$ and $y < 0)$

We already show that $(x > 0$ and $y > 0)$ or $(x < 0$ and $y < 0) \Rightarrow x.y > 0$. Suppose $x.y > 0$. If $x > 0$ and $y < 0$, then $-y > 0$ by (6) so that $-(x.y) = x.(-y) > 0$. This contradicts (6). By symmetry, $y > 0$ and $x < 0$ is also impossible. Hence $x.y > 0 \Rightarrow (x > 0$ and $y > 0)$ or $(x < 0$ and $y < 0)$.

(11) $x > y$ and $z > u \Rightarrow x + z > y + u$

By (5), $x + z > y + z$ and $z + y > u + y$. By (4), $x + z > y + u$.

(12) If $z > 0$, then $x + z > x$. If $z < 0$, then $x + z < x$.

By adding x to both sides, this is a simple consequence of (5). In particular, $x + 1 > x$.

(13) If $x > y$, then

(i) $x.z > y.z$ if $z > 0$

(ii) $x.z < y.z$ if $z < 0$

Now $x - y > 0$.

(i) $x.z - y.z = (x - y).z > 0$ by (1). Hence $x.z > y.z$

(ii) By (6), $-z > 0$. $y.z - x.z = (x - y).(-z) > 0$ by (1). Hence, $y.z > x.z$

(14) If $z > 0$ and $x.z > y.z$, then $x > y$

Now, $x.z > y.z \Rightarrow (x - y).z > 0$. By (10), either $(x - y), z > 0$ or $(x - y), z <0$. Since $z > 0$, then we only can have $x - y > 0$, i.e. $x > y$.

(15) If $z < 0$ and $x.z > y.z$, then $x < y$.

Then $-z > 0$ and since $(-x).(-z) = x.z > y.z = (-y).(-z)$, by (14), we have $-x > -y$. By 13(ii), $x = (-1).(-x) < (-1).(-y) = y$.

(16) $x > 0 \Leftrightarrow x^{-1} > 0$ whenever x^{-1} exists.

Now, $x.x^{-1} = 1 > x.0$. If $x > 0$, by (14), $x^{-1} > 0$. By symmetry, we can then conclude $x > 0 \Leftrightarrow x^{-1} > 0$.

(17) $x > 1 \Leftrightarrow 0 < x^{-1} < 1$ whenever x^{-1} exists.

Since $x > 1 > 0$, by (16), $x^{-1} > 0$. By (13), $1 = x.x^{-1} > x^{-1}$. Similarly, $0 < x^{-1} < 1 \Rightarrow$ $1 = x.x^{-1} < x$ (as $x > 0$) and so the assertion holds.

(18)For $x > 0$,

(i) $x > 1 \Rightarrow x.x > x$
(ii) $x < 1 \Rightarrow x.x < x$
(i) By (13), $x > 1 \Rightarrow x.x > x.1 = x$
(ii) By (13), $x < 1 \Rightarrow x.x < x.1 = x$
Q.E.D

<u>Theorem:</u>

The order $\geq$ on an ordered integral domain (X,+,.,>) is a total order.

For each $m \in X$, $m = m$ and hence $m \geq m$.
Hence $\geq$ is reflexive.

Suppose $m \geq n$ and $n \geq m$. If $n \neq m$, we must have $m > n$ and $n > m$. But this contradict the Trichotomy law for (X,+,.,>).
Hence $\geq$ is anti-symmetric.
Suppose $l \geq m$ and $m \geq n$. If $l = m$ or $n = m$, then it is immediate that $l \geq n$. We hence only consider $l > m$ and $m > n$. But the transitivity law for (X,+,.,>) will give $l > n$, i.e $l \geq n$.
Hence $\geq$ is transitive.
Hence, $\geq$ is a partial order.

Now, take any $m, n \in X$. One of the following must be true: $m>n$(hence $m\geq n$), $m=n$(hence $m\geq n$) or $n>m$ (hence $n\geq m$).

Hence, $\geq$ is also a total order.
Q.E.D

<u>Theorem:</u>

Let (X, +, ., >) be an ordered integral domain. If (X′, +, .) is a subdomain of (X, +, .),then (X′, +, . ,>) is also an ordered integral domain.

Since (X,+,.,>) is an ordered integral domain, there exist a subset P of X s.t
a) $\forall x, y \in P$, $x+y, x.y \in P$
b) $\forall x \in X$, one and only one of the following holds: $x \in P$, $x=0$, $-x \in P$

Define $P'=P\cap X'$. Then
a) $\forall x, y \in P'$,
We have $x+y, x.y\in X'$ since X' is an integral domain. We have $x+y, x.y \in P$ by the defining property of P. Hence, $x+y, x.y \in P'$.
b) For any $x\in X'$, we have $x, 0, -x \in X'$ since X' is an integral domain. By the defining property of P, one and only one of the following holds: $x \in P$, $x=0$, $-x \in P$. Hence, one and only one of the following holds: $x \in P'$, $x=0$, $-x \in P'$.

Hence, (X′, +, .,>) is also an ordered integral domain.
Q.E.D

Note that the following theorem also apply to isomorphism between semi-group and (unordered) integral domain.

<u>Theorem:</u>

The isomorphism $\simeq$ defined on the set of ordered integral domain is an equivalence relation.

(i) Take any ordered integral domain (X, +,.,>).
Define ψ: $X \rightarrow X$ by

$\psi = I_X$.

Clearly, ψ is bijective.

Now, take any x, $y \in X$.

$\psi(x+y) = x+y$

$= \psi(x) + \psi(y)$

$\psi(x.y) = x.y$

$= \psi(x).\psi(y)$

$x>y \Rightarrow \psi(x)>\psi(y)$

Hence, ψ is an isomorphism from $(X, +,.,>)$ to $(X, +,.,>)$ and so $(X, +,.,>) \simeq (X, +,.,>)$. Hence, $\simeq$ is reflexive.

(ii) Let $(X, +,.,>) \simeq (X', +',.',>')$ and let $\phi: X \to X'$ be that isomorphism.

Define $\psi: X' \to X$ by

$\psi = \phi^{-1}$

Clearly, ψ is bijective since ϕ is bijective.

Take any $x', y' \in X'$. Then $\exists$ x, $y \in X$ s.t $\phi(x) = x'$, $\phi(y) = y'$.

$\psi(x'+'y') = \phi^{-1}(\phi(x)+'\phi(y))$

$= \phi^{-1}(\phi(x+y))$

$= I_X(x+y)$

$= x+y$

$= \phi^{-1}(x')+\phi^{-1}(y')$

$= \psi(x')+\psi(y')$

$\psi(x'.'y') = \phi^{-1}(\phi(x).'\phi(y))$

$= \phi^{-1}(\phi(x.y))$

$= I_X(x.y)$

$= x.y$

$= \phi^{-1}(x').\phi^{-1}(y')$

$= \psi(x').\psi(y')$

$x'>'y' \Rightarrow \phi(x)>'\phi(y)$

$\Rightarrow x>y$

$\Rightarrow \phi^{-1}(x')>\phi^{-1}(y')$

$\Rightarrow \psi(x')>\psi(y')$

Hence, ψ is an isomorphism from $(X', +',.',>')$ to $(X, +,.,>)$ and so $(X, +,.,>) \simeq (X', +',.',>') \Rightarrow (X', +',.',>') \simeq (X, +,.,>)$. Hence, $\simeq$ is symmetric.

(iii) Let $(X, +,.,>) \simeq (X', +',.',>')$ and $(X', +',.',>') \simeq (X'', +'',.'',>'')$ and let $\phi_1: X \to X'$, $\phi_2: X' \to X''$ be those isomorphism respectively. Define $\psi: X \to X''$ by

$\psi = \phi_2 \circ \phi_1$

Clearly, ψ is bijective since ϕ_1, ϕ_2 are both bijective.

Take any x, $y \in X$. Then

$\psi(x+y) = \phi_2(\phi_1(x+y))$

$= \phi_2(\phi_1(x)+'\phi_1(y))$

$= \phi_2(\phi_1(x))+''\phi_2(\phi_1(y))$

$= \psi(x)+''\psi(y)$

$\psi(x.y) = \phi_2(\phi_1(x.y))$

$= \phi_2(\phi_1(x).'\phi_1(y))$

$= \phi_2(\phi_1(x)).''\phi_2(\phi_1(y))$

$= \psi(x).''\psi(y)$

$x>y \Rightarrow \phi_1(x)>'\phi_1(y)$
$\Rightarrow \phi_2(\phi_1(x))>''\phi_2(\phi_1(y))$
$\Rightarrow \psi(x)>''\psi(y)$

Hence, ψ is an isomorphism from (X, +,.,>) to (X″, +″,.″,>″) and so (X, +,.,>) $\simeq$ (X′, +′,.′,>′) and (X′, +′,.′,>′) $\simeq$ (X″, +″,.″,>″) $\Rightarrow$ (X, +,.,>) $\simeq$ (X″, +″,.″,>″). Hence, $\simeq$ is transitive.

Hence, $\simeq$ is an equivalence relation on the set of ordered integral domain.

Q.E.D

Theorem:

Let ϕ be any isomorphism from (G, *) to (G′, *′). Then the following holds:

(i) $\phi(e)=e'$

For any $x'\in G'$, $\exists$ $x\in G$ s.t $\phi(x)=x'$, since ϕ is onto. Then

$\phi(e)*'x'=\phi(e)*'\phi(x)$
$=\phi(e*x)$
$=\phi(x)$
$=x'$

Similarly, $x'*'\phi(e)= x'$ and so $\phi(e)=e'$

(ii) $\phi(x^{-1})= (\phi(x))^{-1}$ $\forall$ $x\in G$

$\phi(x^{-1}) *'\phi(x) =\phi(x^{-1}*x)$
$=\phi(e)$
$=e'$

Similarly, $\phi(x)*'\phi(x^{-1})=e'$ and so $\phi(x^{-1})= (\phi(x))^{-1}$

Q.E.D

Theorem:

Let (G, *) be a group. For any non-empty subset G′ of G, (G′, *) is a subgroup of (G, *) iff $\forall x, y\in G'$, $x*y^{-1}\in G'$.

Obviously, if (G′, $*$) is a subgroup of (G, $*$), then for any $x, y\in G'$, we also have $y^{-1}\in G'$ so that $x*y^{-1}\in G'$.

Suppose then that $\forall$ $x, y\in G'$, $x*y^{-1}\in G'$. We check through the four properties.

(i) associativity
This is directly inherited.

(ii) $e\in G'$
Since G′ is non-empty, take $x\in G'$. Then $e = x*x^{-1}(\in G')$.

(iii) $\forall$ $y\in G'$, $y^{-1}\in G'$
Take any $y\in G'$. By (ii), since $e\in G'$ also, we have $y^{-1} = e*y^{-1}(\in G')$.

(iv) G′ is closed under $*$
Take any $x, y\in G'$. By (iii), we have $y^{-1}\in G'$ also. Hence, $x*y = x*(y^{-1})^{-1}(\in G')$ and so G′ is closed under $*$.

Hence (G′, $*$) is a subgroup of (G, $*$).

Q.E.D

Theorem:

Let (X, +, .) be a commutative ring with identity. Then (X, +, .) is an integral domain iff $\forall x, y, z\in X$, $x \neq 0$, $x.y = x.z \Rightarrow y = z$.

Suppose (X, +, .) is an integral domain. Then

$x.y = x.z \Rightarrow x.y - x.z = 0$

$\Rightarrow x.(y - z) = 0$

$\Rightarrow x = 0$ or $y - z = 0$ (by definition of integral domain)

Since $x \neq 0$, we must have $y - z = 0$ so that $y = z$.

Now suppose $\forall$ x, y, z$\in$X, $x \neq 0$, $x.y = x.z \Rightarrow y = z$. Let $x.y = 0$. If $x = 0$, then there is nothing to prove. If $x \neq 0$, then we write $x.y = x.0$ and by the given condition, $y = 0$. Hence (X, +, .) is an integral domain.

Q.E.D

Theorem:

Suppose that

(i) (F, +) is a commutative group.

(ii) (F\{0}, .) is a commutative group

(iii) x.(y+z) =x.y + x.z   ∀x, y, z ∈F

Then (F, +, .) is a field.

First, we check that (F, .) is a semigroup.

(a) closure.

Since we have (ii), we need only check for the case where one of x, y is 0. But that always give x.y=0$\in$F. Hence, F is closed under ..

(b) Associativity

Since we have (ii), we need only check for the case where one of x, y or z is 0. But that always give (x.y).z=0= x.(y.z) so associativity holds in (F, .).

Hence, (F, .) is a semi group. Together with (i) and (iii), we conclude that (F, +, .) is a ring. If one of x, y is 0, then x.y=0=y.x. Together with (ii), this tells us that . is commutative and so (F, +, .) is a commutative ring. The existence of 1 is simply given by (ii). Also, as (F\{0},.) is a group, if x.y=0, then one of x, y must be 0 under closure. Hence, (F, +, .) is also an integral domain. (ii) tells us further that y^{-1} exists
∀ y∈ F\{0} so (F, +, .) is indeed a field.

Q.E.D

Theorem:

Let (X, +, .) be an integral domain. Then for any subset X′ of X, (X′, +, .) is a subdomain of (X, +, .) iff ∀x, y∈X′, 1, x-y, x.y∈X′

If (X′, +, .) is a subdomain, then we obviously have 1, x-y, x.y∈X′ ∀ x, y∈X′. Now suppose the converse. Note that commutativity and associativity of + and . is inherited. Also, X′ is non-empty since 1∈X′. Hence, x-y∈X′ ∀ x, y∈X′ makes (X′, +) a commutative group. x.y∈X′ ∀ x, y∈X′ makes (X′, .) a commutative semi-group. Distributive law is inherited. Since 1∈X′, we can then claim that (X′, +, .) is a commutative ring with unit. As x.y=0⇒ x=0 or y=0 ∀ x, y∈X′ is also inherited,
(X′, +, .) is a subdomain.

Q.E.D

Theorem:

Let (F, +, .) be a field. Then for any subset F′ of F, (F′, +, .) is a subfield of (F, +, .) iff ∀x, y∈F′,we have

(i) 1, x-y∈F′

(ii) $x.y^{-1}$ ∈F′ if y≠0

Suppose (F', +, .) is a subfield. Then obviously, the stated condition holds. Now suppose the converse. Since $1 \in F'$, F' is not empty. Also, note that the distributive law and commutativity of + and . is inherited. Then $x\text{-}y \in F'$ $\forall$ x, $y \in F'$ makes (F', +) a commutative group. Also, $x.y^{-1} \in F'$ $\forall$ x, $y \in F', y \neq 0 \Rightarrow x.y^{-1} \in F'$ $\forall$ x, $y \in F' \backslash \{0\}$. If $x.y^{-1} = 0 = x.0$, then by cancellation law for integral domain, we have $y^{-1} = 0$ which contradict $y \neq 0$. Hence, $x.y^{-1} \in F' \backslash \{0\}$ $\forall$ x, $y \in F' \backslash \{0\}$ so $F' \backslash \{0\}$ is a commutative group. Hence, (F', +, .) is a subfield.

Q.E.D

Theorem:

Let (F, +, ., >) be an ordered field. Then for any x, y∈F, the following holds:

(i) $\mathbf{| r | \geq 0}$

if $r \geq 0$, then $| r | = r \geq 0$. If $r < 0$, then $-r > 0$ and $| r | = -r > 0 \geq 0$.

(ii) $\mathbf{| r | = 0}$ **iff** $\mathbf{r = 0}$

if $r = 0$, then $| r | = r = 0$. If $| r | = 0$, then either $r = | r | = 0$ or $-r = | r | = 0$, i.e. $r = -0 = 0$. Hence, the statement is true.

(iii) $\mathbf{| r | = | -r |}$

if $r = 0$, then $-r = 0$ and so $| r | = 0 = | -r |$ by (ii). If $r > 0$, then $-r < 0$ and so $| r | = r = -(-r) = | -r |$. By symmetry, the case $r < 0$ is also true. Hence, the statement is true.

(iv) $\mathbf{-| r | \leq r \leq | r |}$

If $r \geq 0$, then $| r | = r$. By (i), $-| r | \leq 0$. Hence, $-| r | \leq 0 \leq r = | r |$. Similarly, if $r < 0$, then $| r | = -r$, i.e. $-| r | = r$. Hence, $-| r | = r < 0 \leq | r |$.
Hence, $-| r | \leq r \leq | r |$.

(v) $\mathbf{| x | \leq y}$ **iff** $\mathbf{-y \leq x \leq y}$

Let $| x | \leq y$. Then $0 \leq | x | \leq y$. If $x \geq 0$, then
$-y \leq 0 \leq x \leq | x |$ (by iv)
$\leq y$
If $x \leq 0$, then $-x \geq 0$. Since $| -x | = | x | \leq y$ by (iii), we still have
$-y \leq -x \leq y$, i.e. $y \geq x \geq -y$.
Let $-y \leq x \leq y$. If $x \geq 0$, then $| x | = x \leq y$. If $x < 0$, then $| x | = -x \leq -(-y) = y$.
Hence $| x | \leq y$ iff $-y \leq x \leq y$.

(vi) $\mathbf{| x+y | \leq | x | + | y |}$**, the triangle inequality**

By (iv), $-| x | \leq x \leq | x |$ and $-| y | \leq y \leq | y |$. Hence,
$-(| x | + | y |) \leq x + y \leq | x | + | y |$.
By (v), $| x+y | \leq | x | + | y |$.

(vii) $\mathbf{| r.s | = | r |.| s |}$

If $r \geq 0$, $s \geq 0$, then $r.s \geq 0$. Hence $| r.s | = r.s = | r |.| s |$
If $r < 0$, $s < 0$, then $r.s > 0$. Hence $| r.s | = r.s = (-r).(-s) = | r |.| s |$
If $r < 0$, $s \geq 0$, then $r.s \leq 0$. Hence $| r.s | = -(r.s) = (-r).s = | r |.| s |$
By symmetry, the case $r \geq 0$, $s < 0$ is true.
Hence, $| r.s | = | r |.| s |$

(viii) $\mathbf{| \, | r | - | s | \, | \leq | r - s |}$

By (vi), we have
$| r | = | r - s + s | \leq | r - s | + | s |$, i.e. $| r | - | s | \leq | r - s |$
$| s | = | s - r + r | \leq | s - r | + | r |$, i.e. $-(| r | - | s |) \leq | s - r | = | r - s |$ by (iii).
Hence, $| \, | r | - | s | \, | =$ $| r | - | s | \leq | r - s |$ if $| r | - | s | \geq 0$
$-(| r | - | s |) \leq | r - s |$ if $| r | - | s | < 0$

i.e. $| \, |r| - |s| \, | \leq |r - s|$

(ix) $\mathbf{|r - s| \leq |r| + |s|}$

$|r - s| \leq |r| + |-s|$

$= |r| + |s|$ (by (iii))

(x) **if $\mathbf{y \geq 0}$, $\mathbf{|x| \geq y}$ iff $\mathbf{x \geq y}$ or $\mathbf{x \leq -y}$.**

From (v), we have

$|x| > y \Leftrightarrow x > y$ or $x < -y$

Also,

$|x| = y \Leftrightarrow x = y$ or $-x = y$ i.e $x = -y$

Hence,

$|x| \geq y$ iff $x \geq y$ or $x \leq -y$.

Q.E.D

In the following theorems on sequences, we will always be talking about an ordered field (F, +, ., >).

Theorem:

The limit of a sequence, if it exists, is unique.

Let x and x′ be 2 different limits. We may assume without loss of generality, that $x < x'$. In particular, take $\varepsilon = (x' - x)/2 > 0$.

Since $x_n \to x$, $\exists\, k_1 \in \mathbb{N}$ s.t

$|x_n - x| < \varepsilon \ \forall\, n \geq k_1$

Since $x_n \to x'$, $\exists\, k_2 \in \mathbb{N}$ s.t

$|x_n - x'| < \varepsilon \ \forall\, n \geq k_2$

Take $k = \max\{k_1, k_2\}$. Then $\forall\, n \geq k$,

$|x_n - x| < \varepsilon$, $|x_n - x'| < \varepsilon$

$|x' - x| = |x' - x_n + x_n - x|$

$\leq |x' - x_n| + |x_n - x|$

$< \varepsilon + \varepsilon$

$= x' - x$, a contradiction!

Hence, the limit must be unique.

Q.E.D

Theorem:

If $(x_n) \to x$, then any subsequence of (x_n) also converges to x. Also, (x_n) converges to x iff its k-tail converges to x for some $k \in \mathbb{N}$.

Let (y_n) be any subsequence of (x_n). Given any $\varepsilon > 0$, $\exists\, N \in \mathbb{N}$ s.t

$|x_n - x| < \varepsilon \ \forall\, n \geq N$.

But $y_n = x_i$ for some $i \geq n \ \forall\, n \in \mathbb{N}$ so we may claim

$|y_n - x| < \varepsilon \ \forall\, n \geq N$ also.

Hence, $(y_n) \to x$.

If $(x_n) \to x$, then since any k-tail is also a subsequence, we trivially have some (in fact, all) k-tail converge to x. Conversely, if some k-tail, (y_n), converges to x, then given any $\varepsilon > 0$, $\exists\, N \in \mathbb{N}$ s.t

$|y_n - x| < \varepsilon \ \forall\, n \geq N$

$|x_{n+k-1} - x| < \varepsilon \ \forall\, n \geq N$.

$| x_n - x | < \varepsilon \ \forall\ n \geq N + k - 1$

Hence, $(x_n) \rightarrow x$.

Q.E.D

Theorem:

Any convergent sequence is bounded.

Let $(x_n) \rightarrow x$. In particular, for $\varepsilon = 1$, $\exists\ k \in \mathbb{N}$ s.t

$| x_n - x | < 1 \ \forall\ n \geq k$

i.e. $| x_n | = | x_n - x + x |$

$\leq | x_n - x | + | x |$

$< 1 + | x | \qquad \forall\ n \geq k$

Let $M = \max\{| x_1 |, | x_2 |, ..., | x_{n-1} |, 1 + | x |\}$ and it is clear that

$| x_n | \leq M \ \forall\ n \in \mathbb{N}$, i.e. (x_n) is bounded.

Q.E.D

Theorem:

For any 2 sequences (x_n), (y_n), the following holds:

(i) ***$(x_n) \rightarrow x \Rightarrow (| x_n |) \rightarrow | x |$. Also, $(| x_n |) \rightarrow 0 \Rightarrow (x_n) \rightarrow 0$.***

(ii) ***If $x_n = c \ \forall\ n \in \mathbb{N}$, then $(x_n) \rightarrow c$. We call (x_n) a constant sequence.***

(iii) ***Let $x_n \leq y_n \ \forall\ n \in \mathbb{N}$. If $(x_n) \rightarrow x$ and $(y_n) \rightarrow y$, then $x \leq y$.***

(iv) ***If $(x_n) \rightarrow x$ and M bound (x_n), then $| x | \leq M$***

(i) Given any $\varepsilon > 0$, $\exists\ k \in \mathbb{N}$ s.t

$| x_n - x | < \varepsilon \ \forall\ n \geq k$

But

$\| x_n | - | x \| \leq | x_n - x |$

$< \varepsilon \qquad \forall\ n \geq k$

Hence, $(| x_n |) \rightarrow | x |$ if $(x_n) \rightarrow x$.

Also, if $(| x_n |) \rightarrow 0$, then given any $\varepsilon > 0$, $\exists\ k \in \mathbb{N}$ s.t

$\| x_n | - 0 | < \varepsilon \ \forall\ n \geq k$.

But

$| x_n - 0 | = | x_n |$

$= \| x_n | - 0 |$

$< \varepsilon \qquad \forall\ n \geq k$.

Hence, $(| x_n |) \rightarrow 0 \Rightarrow (x_n) \rightarrow 0$.

(ii) For any $\varepsilon > 0$, take $k = 1$. Then

$| x_n - c | = | c - c |$

$= 0$

$< \varepsilon \qquad \forall\ n \geq k$.

Hence, $(x_n) \rightarrow c$.

(iii) Suppose $x > y$. Then take $\varepsilon = (x - y)/2 > 0$. Then $\exists\ k_1, k_2 \in \mathbb{N}$ s.t

$| x_n - x | < (x - y)/2 \ \ \forall\ n \geq k_1$.

$| y_n - y | < (x - y)/2 \ \ \forall\ n \geq k_2$.

Take $k = \max(k_1, k_2)$. Then $\forall\ n \geq k$, we have

$| x_n - x | < (x - y)/2 \qquad | y_n - y | < (x - y)/2$

$\Rightarrow y - x < 2x_n - 2x < x - y \qquad y - x < 2y_n - 2y < x - y$

$\Rightarrow y + x < 2x_n < 3x - y \qquad 3y - x < 2y_n < x + y$

$\Rightarrow 2y_n < x + y < 2x_n$

i.e. $y_n < x_n$

In particular, $y_k < x_k$ which contradicts $x_k \leq y_k$.

Hence, $x \leq y$.

(iv) By (i), $(| x_n |) \to | x |$. By (ii), the sequence $y_n = M\ \forall\ n \in \mathbb{N}$ converges to M.

Since $| x_n | \leq M = y_n\ \forall\ n \in \mathbb{N}$, (iii) demands that $| x | \leq M$.

Q.E.D

Theorem:

Let (x_n), (y_n) be 2 convergent sequences s.t $(x_n) \to x$, $(y_n) \to y$. Then the following holds:

(i) $(x_n + y_n) \to x + y$

(ii) $(x_n y_n) \to xy$

(iii) If $y \neq 0$, then the sequence (x_n/ y_n) is defined for all $n \geq n_1$, for some $n_1 \in \mathbb{N}$ and this n_1-tail is convergent with limit x/y.

(i) Let any $\varepsilon > 0$ be given. Then $\exists\ k_1, k_2 \in \mathbb{N}$ s.t

$| x_n - x | < \varepsilon/2 \quad \forall\ n \geq k_1$

$| y_n - y | < \varepsilon/2 \quad \forall\ n \geq k_2$

Take $k = \max(k_1, k_2)$ and we have

$| x_n - x | < \varepsilon/2, | y_n - y | < \varepsilon/2 \quad \forall\ n \geq k$.

Hence,

$$\begin{aligned} | (x_n + y_n) - (x + y) | &= | (x_n - x) + (y_n - y) | \\ &\leq | x_n - x | + | y_n - y | \\ &< \varepsilon/2 + \varepsilon/2 \qquad \forall\ n \geq k. \\ &= \varepsilon \qquad \forall\ n \geq k. \end{aligned}$$

Hence, $(x_n + y_n) \to x + y$.

(ii) Now, since (x_n), (y_n) is convergent, they are bounded by some $X, Y \neq 0$ respectively. Let any $\varepsilon > 0$ be given. Then $\exists\ k_1, k_2 \in \mathbb{N}$ s.t

$| x_n - x | < \varepsilon/(2Y) \quad \forall\ n \geq k_1$.

$| y_n - y | < \varepsilon/(2X) \quad \forall\ n \geq k_2$.

Take $k = \max(k_1, k_2)$. Then

$| x_n - x | < \varepsilon/(2Y), | y_n - y | < \varepsilon/(2X)\ \forall\ n \geq k$.

Hence,

$$\begin{aligned} | x_n y_n - xy | &= | x_n y_n - xy_n + xy_n - xy | \\ &\leq | x_n y_n - xy_n | + | xy_n - xy | \\ &= | y_n | | x_n - x | + | x | | y_n - y | \\ &\leq Y| x_n - x | + X| y_n - y | \\ &< Y(\varepsilon/(2Y)) + X(\varepsilon/(2X))\ \forall\ n \geq k. \\ &= \varepsilon \quad \forall\ n \geq k. \end{aligned}$$

Hence, $(x_n y_n) \to xy$.

As a collary, if $(x_n) \to x$, we also have $(cx_n) \to cx$. Just consider the constant sequence $y_n = c\ \forall\ n \in \mathbb{N}$ which obviously converge to c.

(iii) Since $y \neq 0$, take $\varepsilon = | y | > 0$. Then $\exists\ n_1 \in \mathbb{N}$ s.t

$| y_n - y | < | y |\ \forall\ n \geq n_1$

If $y_n = 0$ for some $n \geq n_1$, we will have $| y | = | 0 - y | < | y |$, a contradiction!

Hence, (x_n/ y_n) is well-defined $\forall\ n \geq n_1$ and so we will consider this n_1-tail but for simplicity of notation, still denote it by (x_n/ y_n). Also, (x_n) is bounded by some $X \neq 0$.

Let any $\varepsilon > 0$ be given. Since $|\ y\ | \neq 0$, $\exists\ k_1, k_2 \in \mathbb{N}$ s.t

$|\ y_n - y\ | < (\varepsilon|y|^2)/(4X) \qquad \forall\ n \geq k_1$

$|\ x_n - x\ | < (\varepsilon|y|)/4 \qquad \forall\ n \geq k_2$

Also, $\exists\ k_3 \in \mathbb{N}$ s.t

$|\ y_n - y\ | < |\ y\ |/2 \qquad \forall\ n \geq k_3$

i.e. $|\ y\ | = |\ y - y_n + y_n\ |$

$\leq |\ y - y_n\ | + |\ y_n\ |$

$< |y|/2 + |\ y_n\ | \qquad \forall\ n \geq k_3$

Hence, we have

$|\ y_n\ | > |y|/2$, i.e. $1/|y_n| < 2/|y| \qquad \forall\ n \geq k_3$

Take $k = \max(k_1, k_2, k_3)$. We then have

$|\ y_n - y\ | < (\varepsilon|y|^2)/(4X)$, $|\ x_n - x\ | < (\varepsilon|y|)/4$, $1/|y_n| < 2/|y| \qquad \forall\ n \geq k$

But

$$\begin{aligned}
|\ x_n/y_n - x/y\ | &= |\ (x_ny - xy_n)/(yy_n)| \\
&= (1/|\ yy_n\ |)\ |(x_ny - xy) + (xy - xy_n)| \\
&\leq (1/|\ yy_n\ |)\ (\ |\ x_ny - xy\ | + |\ xy - xy_n|\ ) \\
&= (1/(|y||y_n|\ ))\ (\ |y||\ x_n - x\ | + |x||\ y_n - y\ |\ ) \\
&\leq (1/|\ y_n\ |)\ (\ |\ x_n - x\ | + (X/|y|)|\ y_n - y\ |) \\
&< (2/|y|)\ (\ (\varepsilon|y|)/4 + \ (X/|y|)((\varepsilon|y|^2)/(4x))\ ) \qquad \forall\ n \geq k \\
&\leq (2/|y|)\ (\ (\varepsilon|y|)/4 + (\varepsilon|y|)/4\ ) \\
&= \varepsilon
\end{aligned}$$

Hence, $(x_n/y_n) \to x/y$.

Q.E.D

Squeeze theorem:

Let $(x_n) \to s$, $(z_n) \to s$ and (y_n) be s.t.

$x_n \leq y_n \leq z_n \qquad \forall n \in \mathbb{N}$.

Then (y_n) converges and its limit is also s.

Let any $\varepsilon > 0$ be given. Then $\exists\ k \in \mathbb{N}$ s.t

$|\ x_n - s\ | < \varepsilon$, $|\ z_n - s\ | < \varepsilon \qquad \forall\ n \geq k.$

i.e. $s - \varepsilon < x_n < s + \varepsilon$, $s - \varepsilon < z_n < s + \varepsilon \qquad \forall\ n \geq k.$

Hence, $\forall\ n \geq k$,

$s - \varepsilon < x_n \leq y_n \leq z_n < s + \varepsilon$

$\Rightarrow -\varepsilon < y_n - s < \varepsilon$

i.e. $|\ y_n - s\ | < \varepsilon$

Hence $(y_n) \to s$.

Q.E.D

Theorem:

Every sequence (x_n) has a monotone subsequence.

Consider the set $A = \{n \in \mathbb{N}\ |\ x_n \geq x_m\ \forall\ m \geq n\}$. We have 2 cases:

(i) A is not bounded above

Hence, A is non-empty and so $\exists\ a_1 \in$ A. Define (y_n) as such:

$y_1 = x_{a(1)}$

Suppose $y_n = x_{a(n)}$ for some $a_n \in A$. Since A is not bounded above, $\exists$ $a_{n+1} \in A$ s.t $a_{n+1} > a_n$. Let

$y_{n+1} = x_{a(n+1)}$

Hence (y_n) is a subsequence of (x_n) and by the defining property of A, (y_n) is a decreasing sequence.

(ii) A is bounded above (by k)

Then $n \notin A$ $n > k$. Define (y_n) as such:

$y_1 = x_{k+1}$

Suppose $y_n = x_m$ for some $m>k$. Since $m \notin$ A, $\exists$ $t>m$ ($>k$) s.t $x_t > x_m$. Let

$y_{n+1} = x_t$

Hence (y_n) is a subsequence of (x_n) and we also have (y_n) to be increasing.

Hence, we can always find a monotone subsequence for (x_n).

Q.E.D

Theorem:

Every convergent sequence is also Cauchy.

Let $(x_n) \to x$. Let any $\varepsilon > 0$ be given. Then $\exists$ $k \in \mathbb{N}$ s.t

$| x_n - x | < \varepsilon/2 \quad \forall\ n \geq k.$

For any n, m $\geq$ k, we then have

$$\begin{aligned} | x_n - x_m | &= | (x_n - x) + (x - x_m) | \\ &\leq | x_n - x | + | x - x_m | \\ &< \varepsilon/2 + \varepsilon/2 \\ &= \varepsilon \end{aligned}$$

Hence (x_n) is also Cauchy.

Q.E.D

Theorem:

Every Cauchy sequence is bounded.

Let (x_n) be a Cauchy sequence. Then for $\varepsilon = 1$, $\exists$ $k \in \mathbb{N}$ s.t

$| x_n - x_m | < 1 \quad \forall\ n, m \geq k.$

Hence, for $n \geq k$, we have

$$\begin{aligned} | x_n | &= | x_n - x_k + x_k | \\ &\leq | x_n - x_k | + | x_k | \\ &< 1 + | x_k | \end{aligned}$$

Let $M = \max\{ | x_1 |, | x_2 |, ..., | x_{k-1}|, 1 + | x_k | \}$ and it is clear that $| x_n | \leq M$ $\forall$ $n \in \mathbb{N}$, i.e. (x_n) is bounded.

Q.E.D

Theorem:

If (x_n) is Cauchy, then any subsequence of (x_n) is also Cauchy. Also, (x_n) is Cauchy iff its k-tail is Cauchy for some $k \in \mathbb{N}$.

Let (y_n) be any subsequence of (x_n). Given any $\varepsilon > 0$, $\exists$ $N \in \mathbb{N}$ s.t

$| x_n - x_m | < \varepsilon \quad \forall\ n, m \geq N.$

But $y_n = x_i$ for some $i \geq n$ $\forall$ $n \in \mathbb{N}$ so we may claim

$| y_n - y_m | < \varepsilon \quad \forall\ n, m \geq N$ also.

Hence $(y_n) \to x$

If (x_n) is Cauchy, then since any k-tail is also a subsequence, we trivially have some (in fact, all) k-tail Cauchy also. Conversely, if some k-tail (y_n) is Cauchy, then given any $\varepsilon > 0$, $\exists\ N \in \mathbb{N}$ s.t

$| y_n - y_m | < \varepsilon \quad \forall\ n, m \geq N$

$| x_{n+k-1} - x_{m+k-1} | < \varepsilon \quad \forall\ n, m \geq N$

$| x_n - x_m | < \varepsilon \quad \forall\ n, m \geq N + k - 1$

Hence, (x_n) is Cauchy also.

Q.E.D

Theorem:

Let (x_n) be a Cauchy sequence s.t it is not true that $(x_n) \to 0$. Then $\exists\, M > 0$ s.t $\exists\ n_1 \in \mathbb{N}$ s.t $| x_n | \geq M \quad \forall n \geq n_1$

Suppose not. For any $\varepsilon > 0$, $\exists\ k \in \mathbb{N}$ s.t

$| y_n - y_m | < \varepsilon/2 \quad \forall\ n, m \geq k$

In particular, $\exists\ t > k$ s.t

$| y_t | < \varepsilon/2$ (else $M = \varepsilon/2$ satisfy our claim, contradicting our hypothesis that no such M exists!)

But

$$\begin{aligned} | y_n - 0 | &= | y_n - y_t + y_t | \\ &\leq | y_n - y_t | + | y_t | \\ &< | y_n - y_t | + \varepsilon/2 \\ &< \varepsilon/2 + \varepsilon/2 && \forall\ n \geq t \\ &= \varepsilon && \forall\ n \geq t \end{aligned}$$

i.e. $(y_n) \to 0$, a contradiction!

Hence, such a M must exists.

Q.E.D

Theorem:

Let (x_n) and (y_n) be two Cauchy sequences. Then the following holds:

(i) $(x_n + y_n)$ is Cauchy.

(ii) $(x_n\, y_n)$ is Cauchy.

(iii) If we do not have $(y_n) \to 0$, then some n_1-tail of (x_n/y_n) is well-defined and this n_1-tail is Cauchy.

(i) Let any $\varepsilon > 0$ be given. Then $\exists\ k_1, k_2 \in \mathbb{N}$ s.t

$| x_n - x_m | < \varepsilon/2 \quad \forall\ n \geq k_1$

$| y_n - y_m | < \varepsilon/2 \quad \forall\ n \geq k_2$

Take $k = \max(k_1, k_2)$. Then

$| x_n - x_m | < \varepsilon/2,\ | y_n - y_m | < \varepsilon/2 \quad \forall\ n \geq k.$

But

$$\begin{aligned} | (x_n + y_n) - (x_m + y_m) | &= | (x_n - x_m) + (y_n - y_m) | \\ &\leq | x_n - x_m | + | y_n - y_m | \\ &< \varepsilon/2 + \varepsilon/2 && \forall\ n \geq k. \\ &= \varepsilon && \forall\ n \geq k. \end{aligned}$$

Hence, $(x_n + y_n)$ is also Cauchy.

(ii) Now, since (x_n), (y_n) is Cauchy, they are bounded by some $X, Y \neq 0$. Let any $\varepsilon > 0$ be given. Then $\exists\ k_1, k_2 \in \mathbb{N}$ s.t

$| x_n - x_m | < \varepsilon/(2Y) \quad \forall\ n, m \geq k_1$

$| y_n - y_m | < \varepsilon/(2X) \quad \forall\, n, m \ge k_2$

Take $k = \max(k_1, k_2)$. Then

$| x_n - x_m | < \varepsilon/(2Y) \qquad | y_n - y_m | < \varepsilon/(2X) \quad \forall\, n, m \ge k$

Hence,

$$\begin{aligned} | x_n y_n - x_m y_m | &= | (x_n y_n - x_m y_n) + (x_m y_n - x_m y_m) | \\ &\le | x_n y_n - x_m y_n | + | x_m y_n - x_m y_m | \\ &= | y_n | \, | x_n - x_m | + | x_m | \, | y_n - y_m | \\ &\le Y \, | x_n - x_m | + X \, | y_n - y_m | \\ &< Y(\varepsilon/(2Y)) + X(\varepsilon/(2X)) && \forall\, n, m \ge k \\ &= \varepsilon && \forall\, n, m \ge k \end{aligned}$$

Hence, $(x_n y_n)$ is also Cauchy.

(iii) First, note that since $(y_n) \to 0$ is not true, $\exists\, M > 0$ s.t $\exists\, n_1 \in \mathbb{N}$ s.t

$| y_n | \ge M \quad \forall\, n \ge n_1$

Hence, we consider then only the n_1-tail of (x_n /y_n), but for ease of notation, still denote it by (x_n /y_n). Note that we trivially have $| y_n | \ge M > 0$ so (x_n /y_n) is well-defined.

Note also that (x_n), (y_n) are bounded by $X, Y \neq 0$ respectively.

Hence, given any $\varepsilon > 0$, $\exists\, k_1, k_2 \in \mathbb{N}$ s.t

$| x_n - x_m | < (M^2\varepsilon)/(2Y) \quad \forall\, n, m \ge k_1$

$| y_n - y_m | < (M^2\varepsilon)/(2X) \quad \forall\, n, m \ge k_2$

Take $k = \max(k_1, k_2)$ and we have

$| x_n - x_m | < (M^2\varepsilon)/(2Y), \ | y_n - y_m | < (M^2\varepsilon)/(2X) \quad \forall\, n, m \ge k$

But

$$\begin{aligned} | x_n/y_n - x_m/y_m | &= | (x_n y_m - x_m y_n)/(y_n y_m) | \\ &= (1/(|y_n||y_m|))(|(x_n y_m - y_m x_m) + (y_m x_m - x_m y_n)|) \\ &\le (1/(|y_n||y_m|))(| x_n y_m - y_m x_m | + | y_m x_m - x_m y_n |) \\ &= (1/(|y_n||y_m|))(| y_m | \, | x_n - x_m | + | x_m | \, | y_m - y_n |) \\ &\le (1/ M^2)(Y \, | x_n - x_m | + X \, | y_m - y_n |) \\ &< (1/ M^2)(Y((M^2\varepsilon)/(2Y)) + X((M^2\varepsilon)/(2X))) && \forall\, n, m \ge k \\ &= \varepsilon && \forall\, n, m \ge k \end{aligned}$$

Hence, (x_n /y_n) is also Cauchy.

Q.E.D

Theorem:

Let $(F, +, ., >)$ be an ordered field. Let A be a non-empty subset of F and u be an upper bound of A. Then the following statements are equivalent:

(i) $u = \text{Sup}A$

(ii) For every $\varepsilon > 0$, $\varepsilon \in F$, $\exists x \in A$ s.t $u - \varepsilon < x$.

(iii) For every $x \in F$ s.t $x < u$, $\exists y \in A$ s.t $x < y$.

Suppose (i). Then given any $\varepsilon > 0$, $u - \varepsilon < u = \text{Sup}A$. Hence, $\exists\, x \in A$ s.t $u - \varepsilon < x$, else $x \le u - \varepsilon\ \forall\, x \in A$ which means $u - \varepsilon$ is an upper bound for A and that contradicts $u - \varepsilon < \text{Sup}A$. Hence, (ii) holds.

Suppose (ii). For any $x \in F$ s.t $x < u$, take $\varepsilon = u - x > 0$. Hence, $\exists\, y \in A$ s.t $u - \varepsilon < y$, i.e. $x = u-(u - x) < y$. Hence, (iii) holds.

Suppose (iii). Take any upper bound u' of A s.t $u' < u$. Then $\exists\, x \in A$ s.t $u' < x$. This contradicts u' being an upper bound for A. Hence $u \le u'$ for any upper bound u' of A and so $u = \text{Sup}A$. Hence, (i) holds.

Hence the statements are equivalent.

Q.E.D

Theorem:

Let (F, +, ., >) be an ordered field. Let A be a non-empty subset of F and l be a lower bound of A. Then the following statements are equivalent:

(i) ***$l = \inf A$***

(ii) ***For every $\varepsilon > 0$, $\varepsilon \in F$, $\exists x \in A$ s.t $l + \varepsilon > x$.***

(iii) ***For every $x \in F$ s.t $x > l$, $\exists y \in A$ s.t $x > y$.***

Suppose (i). Then given any $\varepsilon > 0$, $l + \varepsilon > l = \inf A$. Hence, $\exists$ $x \in A$ s.t $l + \varepsilon > x$, else $x \geq l + \varepsilon$ $\forall$ $x \in A$ which mean $l + \varepsilon$ is a lower bound for A and that contradicts $l + \varepsilon > \inf A$. Hence, (ii) holds.

Suppose (ii). For any $x \in F$ s.t $x > l$, take $\varepsilon = x - l > 0$. Hence, $\exists$ $y \in A$ s.t $l + \varepsilon > y$, i.e. $x = l + (x - l) > y$. Hence, (iii) holds.

Suppose (iii). Take any lower bound l' of A s.t $l' > l$. Then $\exists$ $x \in A$ s.t $l' > x$. This contradicts l' being a lower bound for A. Hence $l \geq l'$ for any lower bound l' of A and so $l = \inf A$. Hence, (i) holds.

Hence the statements are equivalent

Q.E.D

Theorem:

Let (F, +, ., >) be an ordered field with the least upper bound property. Let A and B be non-empty subsets of F. Let $-A = \{-x \mid x \in A\}$, $x + A = \{x + y \mid y \in A\}$, $A + B = \{x + y \mid x \in A, y \in B\}$, $xA = \{ xy \mid y \in A\}$, $AB = \{xy \mid x \in A, y \in B\}$. Then the following holds:

(i) ***A is bounded above iff –A is bounded below and in that case –SupA = inf(-A). As a result, (F,+,.,>) must also be order complete.***

(ii) ***If A and B are both bounded above, then Sup(A + B) = SupA + SupB***

(iii) ***If A and B are both bounded above and $x, y > 0$ $\forall x \in A, y \in B$, then Sup(AB) = SupASupB.***

(iv) ***SupA $\geq$ SupB if A $\supseteq$ B and A is bounded above.***

(i) Let A be bounded above by some u. Then $x \leq u$ $\forall$ $x \in A$, i.e. $-x \geq -u$ $\forall$ $x \in A$ and so –A is bounded below (by –u). Similarly, if –A is bounded below by some l, then we have $x \geq l$ $\forall$ $x \in -A$, i.e. $-x \leq -l$ $\forall$ $x \in -A$ and so A is bounded above (by $-l$).

In such a case (i.e. if A is bounded above), SupA exists and since SupA is an upper bound of A, we have shown –SupA is a lower bound for –A. For every $\varepsilon > 0$, $\exists$ $x \in A$ s.t SupA – $\varepsilon < x$, i.e. –SupA + $\varepsilon > -x$ ($\in -A$). Hence, –SupA = inf(-A).

Now, by simply noting that A =-(-A), the preceding result immediately tells us that for any non-empty subset A that is bounded below, we must have inf(A)= - Sup(-A), i.e inf(A) exist. Hence, (F,+,.,>) also has the greatest lower bound property and so is order complete.

(ii) Since A and B are both bounded above, SupA, SupB exist. For any $x + y \in A + B$, we have $x \leq$ SupA, $y \leq$ SupB and so $x + y \leq$ SupA + SupB, i.e. SupA + SupB is an upper bound for A + B. Given any $\varepsilon > 0$, $\exists$ $x \in A$, $y \in B$ s.t

SupA – (ε/2) < x, SupB – (ε/2) < y,

i.e. (SupA + SupB) – ε = (SupA – (ε/2)) + (SupB – (ε/2)) < x + y ($\in$ A + B).

Hence, Sup(A + B) = SupA + SupB.

As a consequence, Sup(x + A) = x + SupA. Just consider the set B = {x} where SupB = MaxB = x trivially.

(iii) Since A and B are both bounded above, SupA, SupB exist. For any $xy\in AB$, we have $0 < x \le$ SupA, $0 < y \le$ SupB and hence $xy \le$ SupASupB, i.e. SupASupB is an upper bound for AB. Note that since $A, B \neq \phi$, $\exists\, x\in A, y\in B$ s.t SupA $\ge x > 0$, SupB $\ge y > 0$, i.e. SupA, SupB > 0.

Let any $\varepsilon > 0$ be given. Let

$\varepsilon_1' = \varepsilon/(2\text{SupB}) > 0$, $\varepsilon_2' = \varepsilon/(2\text{SupA}) > 0$

and take $\varepsilon_1 = \min(\text{SupA}, \varepsilon_1')$, $\varepsilon_2 = \min(\text{SupB}, \varepsilon_2')$. Hence, $\exists\, x\in A, y\in B$ s.t

$0< \text{SupA} - \varepsilon_1 < x \qquad 0< \text{SupB} - \varepsilon_2 < y$

$\Rightarrow (\text{SupA} - \varepsilon_1)(\text{SupB} - \varepsilon_2) < xy$

$\Rightarrow \text{SupASupB} - \varepsilon_2\text{SupA} - \varepsilon_1\text{SupB} + \varepsilon_1\varepsilon_2 < xy$

$\Rightarrow \text{SupASupB} - \varepsilon_2\text{SupA} - \varepsilon_1\text{SupB} < xy \qquad (\because \varepsilon_1\varepsilon_2 > 0)$

$\Rightarrow \text{SupASupB} - \varepsilon_2'\text{SupA} - \varepsilon_1'\text{SupB} < xy \qquad (\because \varepsilon_1 < \varepsilon_1', \varepsilon_2 < \varepsilon_2')$

$\Rightarrow \text{SupASupB} - (\varepsilon/(2\text{SupA}))\text{SupA} - (\varepsilon/(2\text{SupB}))\text{SupB} < xy$

$\Rightarrow \text{SupASupB} - \varepsilon < xy\ (\in AB)$

Hence, Sup(AB) = SupASupB.

As a consequence, Sup(xA) = xSupA if $x > 0$. Just consider the set $B = \{x\}$ where SupB = MaxB = x trivially.

(iv) First, observe that if u is an upper bound of A, then $u \ge x\ \forall\, x\in A$ (and hence $\forall\, x\in B$ since $B \subseteq A$) and so u is an upper bound for B also. Now A is bounded above so SupA exists. As SupA is an upper bound for A, we have argued that SupA is also an upper bound for B and so SupB exists. Furthermore, by the definition of suprema, we immediately have SupA $\ge$ SupB.

Q.E.D

End Of General Proof Section

CHAPTER 1: THE NATURAL NUMBERS SYSTEM

Introduction

Our basic foundation is the natural numbers which we will create using Peano's axioms. Intuitively, the natural numbers poses no conceptual difficulty, as they are indeed *very natural*. We have no difficulty accepting that 3 and 5 makes 8 and in fact can easily give a 'physical proof' by putting 3 apples and 5 apples into a basket and with a casual wave of the hand, beg the audience to *count* the number of apples in the basket. Certainly, they will all end up with the answer 8. We can also 'prove' 3 multiplied by 4 gives the number 12 by taking 3 plates each containing 4 cakes and then *count* the total number of cakes altogether. Notice that the process of counting is always involved, and this should gives us an idea that the essence of the natural number is counting!

This chapter attempts to demonstrate how the natural number system can be built up purely on Peano's axioms. Intuitively, we can claim that Peano's axioms assumed basically only the 'process of counting'. Hence, we simply blatantly stated that mankind has the natural ability to count, and leave it at that. What is our justification for starting from this assumption? Why do we not start from formal set theory, or maybe simply assumed the ability to add instead of counting?

Our contention is that counting is indeed a very natural process to man. Formal set theory is too abstract, and hence does not really serves our purpose in creating an intuitive number system supported by rigorous mathematics. Why then is counting favored over addition? After all, both appear natural and relate equally well to the average human. To answer this, we have to look back to our elementary schooling and recall how we are taught counting and addition.

Ask a little kid what follows 8 and he will immediately(*hopefully*) say the answer 9. Ask him what is the sum of 8 and 1 and a slight lag in response should be detected. The assumption behind this conclusion is that answers stored in memory is retrieved faster than answers that require some sort of computation. Has any elementary teacher ever impart to his student the method of obtaining the number that follows 8? Of course not! One simply memorize that 9 follows 8. In contrast, we are able to learn a method that allows us to add and so we are able to get the sum of 7 and 9 even though we have not memorized that the answer is 16. Hence, counting is more elementary and in fact, it can never be learned! The world does not collapse if 10 follows 8. It is just a change of symbol. The world will undergo an earthquake if 1+2 is 3 and 1+ 3 is 2 simultaneously. It is no longer a matter of symbols. This particular addition method just does not express the conventional notion of addition. This means that what was taught as counting is really an agreement on convention. Viewed from another angle, this means that nobody can really teach us to count and so the ability to count must be innate! Hence, Peano's axioms assumed an innate human ability and can anybody really have any arguments against such an assumption?

For those readers bored with all these philosophical castle building, rest assured that they are really irrelevant and does not affect our technical construction in the least. We move on formally to Peano's axioms.

The five axioms of Peano

Defn: We assume the existence of a set $\mathbb{N}$ with the following properties:

N(i) There exists an element $1\in\mathbb{N}$

N(ii) For every $n\in\mathbb{N}$, there exists an element $S(n)\in\mathbb{N}$ such that

$\{(n,S(n))|\ n\in\mathbb{N}\}$ is a function.

N(iii) $1\notin S(\mathbb{N})$

N(iv) S is one-one.

N(v) If P is any subset of $\mathbb{N}$ such that $1\in P$ and $S(n)\in P\ \forall\ n\in P$, then

$P=\mathbb{N}$.

Let us discuss the five axioms informally and see how it relates to our familiar natural number system. First of all, N(i) tells us that the set has at least an element, which we call 1. This 1 is meant to represent the familiar *one* and we shall see further how the rest of the axioms guarantee that. N(ii) is rather an inductive process. Since we already have 1 in the set, we can use N(ii) to generate S(1), which we call 2, and from 2 we create S(2) and so forth. We call S the **successor function** and S(n) the **successor** of n. The successor of an element can be viewed intuitively as the 'next' element, giving rise to the concept of counting. N(iv) says that S is one-one. Hence, since S is defined to be a one-one function, we have ensured that there is one and only one successor for every n in the set. Notice how our familiar number system is already taking shape through N(i), N(ii), and N(iv) alone. N(iii) says that 1 is not the successor of any element in the set and it is this crucial axiom (and not N(i)) that sets 1 apart from the rest. We may just as well postulate any other element in N(i) and its purpose would serve equally well. But if we do so, we would still have to postulate the existence of 1 in some other axioms to make the set resemble our familiar number system so we might as well use 1 to serve a dual purpose. It is N(iii) that tells us that 1 is our 'beginning' element and that there is nothing 'before' it. N(v) is the familiar mathematical induction, which we so often use. Instead of assuming P_k is true and proceeding to prove the statement P_{k+1}(the binary operation + has not been defined yet!), we will usually define a subset of $\mathbb{N}$,

$P=\{n\in\mathbb{N}|$ n belongs to P iff n satisfy some property $P_n\}$.

If P satisfy N(v), then N(v) guarantee that $P=\mathbb{N}$, i.e, the statement P_n is true $\forall\ n\in\mathbb{N}$. The logic remains the same, the only difference being that we try to prove things in an axiomatic way.

We will denote any such system by $(\mathbb{N},1,S)$, $\mathbb{N}$ being a name for the set, 1 being a name for that element which satisfy N(iii) and S being a name for that function from $\mathbb{N}$ to $\mathbb{N}$ which satisfy N(ii),N(iii) and N(iv). Note that we have only assumed the existence of some set that satisfy all five axioms. Until now, nothing prevent the existence of some other set, together with its own successor function, which may have radically different properties from the first, that also satisfy all 5 axioms. In particular, it may seem that even for a fixed set $\mathbb{N}$, we can define several, perhaps limitless, different successor functions. Suppose a different system called (ResidentOfSingapore, President, Rank) does exist. Then our system would not be unique. We therefore cannot say that this is a good representation for our natural number system since it can spawn off plenty other different systems with different properties.

Hence, we now introduce the concept of **isomorphism** for natural number systems. Formally,

Defn*:* Let ($\mathbb{N}$,1,S) and ($\mathbb{N}'$,1′,S′) be two natural number systems satisfying N(i) to N(v). We say $\mathbb{N}$ and $\mathbb{N}'$ are isomorphic if there exists a bijective function

$\phi: \mathbb{N} \to \mathbb{N}'$ such that

(i) $\phi(1)=1'$

(ii) $\phi\circ S(n)=S'\circ\phi(n)\ \forall\ n\in\mathbb{N}$.

But what does isomorphism between 2 natural number systems really means? Take any natural number system ($\mathbb{N}$,1,S) for instance. This system would have certain elements in it, contained in the set $\mathbb{N}$. In particular, 1 is rather special but why is it so special? On retrospection, the only other thing about this system is that there is a structure S imposed on it. S forces a relationship between the elements in $\mathbb{N}$. In fact, we can even say that the nature of the element depends totally on the nature of S. We can label 1 as apple but nothing would have much changed. It is just that now we have to write S(apple)=2, and that apple is not the successor of any elements in $\mathbb{N}$. But if we tell everybody that 1 has been renamed as apple, then essentially nothing would have changed. If we say that two natural number systems are isomorphic, then it must be possible for us to rename all the elements in one system using the names of the elements in the other system. But it is not just any renaming. We must make sure that the structure is preserved also. That is to say, we can rename n in $\mathbb{N}$ as some element say, n′ in $\mathbb{N}'$, but if we do so, then we are also forced to rename the successor of n using the name of the successor of n′. If we can do this for every element in $\mathbb{N}$, then we can roughly see that S and S′ are really quite identical structures, just that they are applied to different sets of elements. Hence, if there exist ϕ, which is essentially a sort of renaming function, from $\mathbb{N}$ to $\mathbb{N}'$ that satisfy the criteria of isomorphism:

(0) it is one-one and onto

This will make sure that every element in one system is matched up with one and only one element in the other.

(i) $\phi(1)= 1'$

Now, the element 1 is really special under S in the sense that no other element in $\mathbb{N}$ has its properties. Hence, 1 must at least be matched with 1′ if the structure is to have any hope of being preserved. Also, this is an essential criterion since it is not a consequence of (ii)

(ii) $\phi\circ S(n)=S'\circ\phi(n)\ \forall\ n\in\mathbb{N}$

This is the criterion, together with (i) that assures us that the renaming preserves the structure also. S essentially has only one effect on each element, n, in $\mathbb{N}$. That is, it ties up some other element m in $\mathbb{N}$ to be n's successor. If after renaming, m′ is still n′'s successor under S' in $\mathbb{N}'$, then things are really just as before, except that everybody may have different names now.

We now see why the definition of isomorphism is as such. It is essentially a set of criteria that helps us to see if the difference between 2 natural number systems is really only a matter of symbols. If that is so, then one is as good as the other since nobody would really argue that Peter has changed into another person if he just decide to change his name to Gary.

If all natural number systems happen to be isomorphic, then we would be justified in using the set spawned by the five axioms as a model for our familiar natural number system. We will proceed to prove this fact after we proved the **iteration theorem**, which will shorten many proofs considerably once it is established and can be appealed to.

Iteration theorem

Let ($\mathbb{N}$, 1, S) be any natural system and B be any non-empty set. Given $b\in B$ and a function $\psi: B\to B$, $\exists$ an unique function $\phi: \mathbb{N}\to B$ such that $\phi(1) = b$ and $\phi(S(n))= \psi(\phi(n))\ \forall\ n\in\mathbb{N}$.

We need only to establish the existence of a non-empty set $E \subseteq \mathbb{N}\times B$ which has the following properties:

(i) If $(n, m), (n, m') \in E$, then $m = m'$.
This is just another way of saying E is a function in coordinate notation.

(ii) $(1, b) \in E$
Incidentally, this also ensures that E is non-empty.

(iii) If $(n, m) \in E$, then $(S(n), \psi(m)) \in E$.

First, note that $\mathbb{N}\times B$ has properties:

(ii) Since $1\in \mathbb{N}$, $b\in B$, we obviously have $(1, b) \in \mathbb{N}\times B$

(iii) Observe that $(S(n), \psi(m)) \in \mathbb{N}\times B\ \forall\ n\in \mathbb{N}$, $m\in B$ so (iii) is always true for $\mathbb{N}\times B$.

Now, let F denote the set of all subset of $\mathbb{N}\times B$ which has properties (ii) and (iii). Then F is non-empty since $\mathbb{N}\times B\in F$. Let E be the intersection of all elements in F. We claim that E has the property (i) and that $E\in F$ also, hence proving the existence of ϕ.

Since $(1, b)\in F_i\ \forall\ F_i\in F$, $(1, b)\in E$ and so E has property (ii).

Suppose $(n, m)\in E$, then $(n, m)\in F_i\ \forall\ F_i\in F$. By hypothesis, we then have $(S(n), \psi(m)) \in F_i$ for each $F_i\in F$. Therefore, $(S(n), \psi(m)) \in E$ and so E has property (iii).

Hence, $E\in F$.

Let $P = \{n\in \mathbb{N} \mid (n, m), (n, m')\in E \Rightarrow m = m'\}$ Now, $(1, b)\in E$. Suppose $(1, b_2) \in E$ also and $b\neq b_2$. Consider the set $E'=E/(1, b_2)$. Obviously, E' has property (ii). Since E already has property (iii), E' also has property (iii) for the simple reason that we removed only $(1, b_2)$ from E and (iii) is not violated since 1 is not the successor of any $n\in \mathbb{N}$. Hence, $E'\in F$. But $E \subseteq F_i\ \forall\ F_i\in F$. Since $E'\subseteq E$, this mean $E = E'$ which is a contradiction. Hence $1\in P$. Suppose $n\in P$. Then $(n, m), (n, m')\in E \Rightarrow m = m'$. If $(S(n), l), (S(n), l') \in E$ but $l \neq l'$, then we claim there does not exist simultaneously $m, m'\in B$ s.t. $(n, m), (n, m')\in E$ and $\psi(m) = l$, $\psi(m') = l'$. For if this situation occur, we must then have m = m′ so that $l = l'$ (since ψ is a function), contradicting $l \neq l'$. Hence we can safely remove at least an element, say (S(n), l) so that E′ = E\(S(n), l) retain property (iii). Since E′ obviously has property (ii), E′∈F. But this forces E′ = E, which is not possible, hence S(n) ∈P whenever n∈P. Therefore, by N(v), P = ℕ and so E also has property (i). Hence, we establish the existence of ϕ.

Now suppose that ϕ and ϕ' are 2 functions satisfying (ii) and (iii). Let P = {n∈ℕ | $\phi(n) = \phi'(n)$}. Then 1∈P since $\phi(1) = b = \phi'(1)$. Suppose n∈P. Then

$$\begin{aligned}\phi(S(n)) &= \psi(\phi(n)) \\ &= \psi(\phi'(n)) \quad (\text{ Since } \phi(n) = \ \phi(n')) \\ &= \phi'(S(n))\end{aligned}$$

Hence S(n)∈P whenever n∈P. By N(v) again, P=ℕ and so ϕ is unique.
Q.E.D

What is this theorem which we have just proved? Well, it simply means that we can recursively use the given function ψ on B to create a function ϕ from ℕ to B. This sort of show that a natural number system satisfying the Peano axioms can be used for 'counting' and that S is a sort of counting function. Notice that we can in a sense count the number of iteration of ψ on b by referring to its correspondence in ℕ through the function ϕ. For example, $\phi(S\circ S(1))= \psi\circ\psi(b)$ which means that ψ is reiterated on b 3 times(counting b itself as one iteration). Furthermore, the fact that ϕ is unique says that there exist essentially only one such way of counting, i.e., counting by relying on the natural structure that S has already imposed on ℕ. We will find this theorem very useful in future proofs.

With the help of the iteration theorem, we are now able to show quite elegantly that Peano's axioms gives us only one type of system.

Theorem: Uniqueness of the natural number system

Let (ℕ, 1, S) and (ℕ′, 1′, S′) be two natural number system. Then (ℕ, 1, S) is isomorphic to (ℕ′,1′,S′).

By the iteration theorem with (ℕ, 1, S) as the natural number system, B = ℕ′, b = 1′, ψ = S′, ∃ an unique function ϕ_1: ℕ→ℕ′ s.t $\phi_1(1) = 1'$ and $\phi_1(S(n)) = S'(\phi_1(n))$ ∀ n∈ℕ.

Similarly, ∃ a unique function ϕ_2 :ℕ′→ℕ s.t $\phi_2(1')= 1$ and $\phi_2(S'(n')) = S(\phi_2(n'))$ ∀ n′∈ℕ′.

Note that ϕ_1 has already satisfy (i) and (ii) of the definition of isomorphism. We need only show that ϕ_1 is bijective. To do so, we show that $\phi_1\circ\phi_2 = I_{ℕ'}$ and $\phi_2\circ\phi_1 = I_{ℕ}$. Let P = {n∈ℕ | $\phi_2\circ\phi_1(n)= n$}. Then 1∈P since $\phi_2\circ\phi_1(1) = \phi_2(1') = 1$. Suppose n∈P. Now,

$$\begin{aligned}\phi_2\circ\phi_1(S(n)) &= \phi_2(S'(\phi_1(n)) \\ &= S(\ \phi_2(\phi_1(n))\ ) \quad (\text{since } \phi_1(n) \in ℕ') \\ &= S(n) \quad (\text{since } \phi_2\circ\phi_1(n) = n \text{ as } n\in P)\end{aligned}$$

Hence S(n) ∈P whenever n∈P. By N(v), P=ℕ and so $\phi_2\circ\phi_1= I_{ℕ}$.

By symmetry $\phi_1\circ\phi_2 = I_{ℕ'}$ and hence ϕ_1 is bijective.

Hence, (ℕ, 1, S) is isomorphic to (ℕ′,1′,S′).

Q.E.D

Notice that the iteration theorem is a sort of comparison between a natural number system and some other arbitrary 'single function' system(we can always view ψ as a structure that is imposed on B). Hence, in the proof, we deliberately choose another natural number system as the arbitrary system, and the iteration theorem should perform the function of matching them up very nicely.

Since all natural number systems are isomorphic and we have assumed the existence of at least one such system, it follows that there is essentially only one such unique natural number system. Any other such system that we can conceive of are but fanciful renaming of this unique natural number system. With appropriate matching, which is always possible as demonstrated by the above theorem, we find that the two systems would be totally indistinguishable. Hence, we can now adopt the convention of labeling *the natural number system* as (ℕ,1,S) and the elements in ℕ will be symbolized by returning to them their familiar notation. That is, we shall name S(1) as 2, S∘S(1) as 3 and so on and so forth. This is hardly the end of the story, though, since we have not really developed any rules to operate with the elements and the natural number system as it stand now is something like a pile of materials and a blueprint. Before we rush into following the blueprint, it would be prudent to develop some elementary properties of ℕ.

Theorem: Elementary properties of ℕ

We prove here some of the elementary properties of ℕ which may prove useful in future developments. We list first the five axioms of Peano.

N(i) There exists an element 1∈ℕ

N(ii) For every n∈ℕ, there exists an element S(n) ∈ℕ such that {(n,S(n))| n ∈ℕ} is a function.

N(iii) 1∉ S(ℕ)

N(iv) S is one-one.

N(v) If P is any subset of ℕ such that 1∈P and S(n)∈P ∀ n∈P, then P=ℕ.

N(vi) ℕ is infinite

Now, by N(iv), S is one-one. Furthermore, 1∉S(ℕ) by N(iii) so S is onto some proper subset of ℕ. Hence, ℕ is infinite.

N(vii)S(n)≠n ∀ n∈ℕ

Let P={n∈ℕ| S(n)≠n}. Then 1∈P since by N(iii), 1∉S(ℕ). Suppose n∈P. If S(S(n))=S(n), then S(n)=n since S is one-one, contradicting n∈P. Hence S(n)∈P whenever n∈P. By N(v), S(n)≠n ∀ n∈ℕ.

N(viii)For every n∈ℕ/{1}, ∃ m∈ℕ such that n=S(m).

Let P={n∈ℕ| n=1 or ∃ m∈ℕ s.t n=S(m)}. 1∈P by definition. Suppose n∈P. If n=1, then S(n)=S(1) and hence belong to P since 1∈ℕ. Otherwise, i.e. if n≠1, we still have S(n)∈P since n∈ℕ. Hence, S(n)∈P whenever n∈P. By N(v), P=ℕ. Now take any

$n\in\mathbb{N}$. If $n\neq 1$, then since $n\in P$, it follows from the defining property of P that $\exists$ $m\in\mathbb{N}$ s.t $n=S(m)$.

N(ix) If $n\in\mathbb{N}$, then $n=1\Leftrightarrow n\notin S(\mathbb{N})$.

$n=1\Rightarrow n\notin S(\mathbb{N})$ follows directly from N(iii).

If $n\notin S(\mathbb{N})$, then since

(i) $1\notin S(\mathbb{N})$ (by N(iii))

(ii) $n\in S(\mathbb{N})$ $\forall$ $n\in\mathbb{N}/\{1\}$ (by N(viii))
it follows that $n=1$.

Hence, $n=1\Leftrightarrow n\notin S(\mathbb{N})$.

Q.E.D

Binary operation on ℕ

We will now define binary operations on the set ℕ which will give it a structure more complex and useful than S alone. After this section, we will be able to add, multiply and even take the exponent of natural numbers. We will say more about the binary operations and their relation with S at the end of the section.

Theorem: Addition

$\exists$ an unique function A: $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ with the following properties:

A(i) $A(n, 1) = S(n)$ $\forall n\in\mathbb{N}$.

A(ii) $A(n, S(m)) = S(A(n, m))$ $\forall n, m\in\mathbb{N}$.

Let any $n\in\mathbb{N}$ be given. By the iteration theorem with $\mathbb{N}$=B, $S(n) = b$, $\psi = S$,

$\exists$ an unique function A_n: $\mathbb{N}\to\mathbb{N}$ s.t $A_n(1) = S(n)$ and $A_n\circ S(m) = S\circ A_n(m)$ $\forall$ $m\in\mathbb{N}$.

Define A: $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ by $A(n, m) = A_n(m)$. A has property A(i) since
$A(n, 1) = A_n(1) = S(n)$ $\forall$ $n\in\mathbb{N}$. A has property A(ii) since for each $n\in\mathbb{N}$,

$$\begin{aligned}A(n, S(m)) &= A_n(S(m))\\ &= S(A_n(m))\\ &= S(A(n, m)) \ \forall\ m\in\mathbb{N}.\end{aligned}$$

Hence $A(n, S(m)) = S(A(n, m))$ $\forall$ $n, m\in\mathbb{N}$. If A is not a function, then $\exists$ $((n, m), l_1)$, $((n, m), l_2)$ $\in A$ s.t $l_1\neq l_2$. But this imply $A_n(m) = l_1\neq l_2 = A_n(m)$, contradicting A_n being a function.

Hence, $\exists$ a function A: $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ with properties A(i), A(ii).

Now, let A′ be another function with properties A(i), A(ii) and for every $n\in\mathbb{N}$, let
$P = \{m\in\mathbb{N}\,|\,A(n, m) = A'(n, m)\}$.
Then $1\in P$ since $A(n, 1) = S(n) = A'(n, 1)$.
Suppose $m\in P$. Then

$$\begin{aligned}A(n, S(m)) &= S(A(n,m))\\ &= S(A'(n, m)) \ \text{(since } m\in P\Rightarrow A(n, m)=A'(n, m))\\ &= A'(n, S(m))\end{aligned}$$

Hence $S(m) \in P$ whenever $m \in P$ and by N(v), $P = \mathbb{N}$. Therefore,
$A(n, m) = A'(n, m)\ \forall\ n, m \in \mathbb{N}$ and so A is unique.

Q.E.D

From now on, we will denote A(n, m) as n+m.

Theorem: Properties of addition

A(i) $\mathbf{S(n) = n + 1\ \forall\ n \in \mathbb{N}}$**.**

A(ii) $\mathbf{n + (m+1) = (n+m) + 1\ \forall\ n, m \in \mathbb{N}}$**.**

A(iii) $\mathbf{1 + n = n + 1\ \forall\ n \in \mathbb{N}}$**.**

Let $P = \{n \in \mathbb{N} \mid 1 + n = n + 1\}$. Then $1 \in P$
since $1 + 1 = 1 + 1$. If $n \in P$, then

$$\begin{aligned} 1 + S(n) &= 1 + (n+1) && \text{(by A(i))} \\ &= (1+n) + 1 && \text{(by A(ii))} \\ &= (n+1) + 1 && \text{(since } n \in P) \\ &= S(n) + 1 \end{aligned}$$

Hence $S(n) \in P$ whenever $n \in P$. By N(v), $P = \mathbb{N}$ and so
$1 + n = n + 1\ \forall\ n \in \mathbb{N}$.

A(iv) $\mathbf{(m+1) + n = (m+n) + 1\ \forall\ n, m \in \mathbb{N}}$**.**

For each $m \in \mathbb{N}$, define

$P = \{n \in \mathbb{N} \mid (m+1) + n = (m+n) + 1\}$
Then $1 \in P$ since $(m+1) + 1 = (m+1) + 1$. If $n \in P$, then

$$\begin{aligned} (m+1) + S(n) &= (m+1) + (n+1) \\ &= ((m+1) + n) + 1 && \text{(by A(ii))} \\ &= ((m+n) + 1) + 1 && \text{(since } n \in P) \\ &= (m + (n+1)) + 1 && \text{(by A(ii))} \\ &= (m + S(n)) + 1 \end{aligned}$$

Hence, $S(n) \in P$ whenever $n \in P$. By N(v), $P = \mathbb{N}$ and so
$(m+1) + n = (m+n) + 1\ \forall\ n, m \in \mathbb{N}$.

A(v) $\mathbf{m + n = n + m\ \forall\ n, m \in \mathbb{N}}$**, the commutative law of addition.**

For each $m \in \mathbb{N}$, define

$P = \{n \in \mathbb{N} \mid m + n = n + m\}$.
By A(iii), $1 \in P$. If $n \in P$, then

$$\begin{aligned} m + S(n) &= m + (n+1) \\ &= (m+n) + 1 && \text{(by A(ii))} \\ &= (n+m) + 1 && \text{(since } n \in P) \\ &= (n+1) + m && \text{(by A(iv))} \\ &= S(n) + m \end{aligned}$$

Hence $S(n) \in P$ whenever $n \in P$. By N(v), $P = \mathbb{N}$ and so the commutative law for addition holds.

A(vi) $\mathbf{(m + n) + k = m + (n + k)\ \forall\ n, m, k \in \mathbb{N}}$**, the associative law of addition.**

For every $n, m \in \mathbb{N}$, define

$P=\{k\in \mathbb{N} \mid (m+n)+k= m+(n+k)\}$
$1\in P$ follow directly from P(ii). If $k\in P$, then

$$\begin{aligned}(m+n)+S(k) &= (m+n)+(k+1)\\ &= ((m+n)+k)+1 \quad \text{(by A(ii))}\\ &=(m+(n+k))+1 \quad \text{(since } k\in P)\\ &=m+((n+k)+1) \quad \text{(by A(ii))}\\ &=m+(n+(k+1)) \quad \text{(by A(ii))}\\ &=m+(n+S(k))\end{aligned}$$

Hence $S(k)\in P$ whenever $k\in P$. By N(v), $P=\mathbb{N}$ and so the associative law for addition holds.

A(vii) $n \neq n + m\ \forall\ m, n\in \mathbb{N}$.

For each $m\in \mathbb{N}$, define

$P = \{n\in \mathbb{N} \mid n \neq n + m\}$.

Obviously, $1 \neq S(m) = 1 + m$ by N(iii). Hence $1\in P$

Suppose $n\in P$. Then

$S(n) \neq S(n+m)$ (since S is one-one and $n \neq n + m$ as $n\in P$)

$$\begin{aligned}\text{But } S(n+m) &= (n+m) + 1\\ &= (n+1) + m\\ &= S(n) + m\end{aligned}$$

Hence $S(n) \neq S(n) + m$ and so $S(n)\in P$ whenever $n\in P$. By N(v), $P = \mathbb{N}$ and so

$n \neq n + m\ \forall\ m, n\in \mathbb{N}$.

A(viii) $n + k = n + m \Rightarrow k = m\ \forall\ m, n, k\in \mathbb{N}$, the cancellation law for addition.

Let $P = \{n\in \mathbb{N} \mid n + k = n + m \Rightarrow k = m\ \forall\ m, k\in \mathbb{N}\}$
Since S is one-one, $k \neq m\Rightarrow 1 + k \neq 1 + m$

i.e., $1 + k = 1 + m\Rightarrow k = m\ \forall\ m, k \in \mathbb{N}$.
Hence $1\in P$.
Suppose $n\in P$. Then

$S(n) + k = S(n) + m$
$\Rightarrow (n+k) + 1 = (n+m) +1$
$\Rightarrow\ n + k = n + m$ (since S is one-one)
$\Rightarrow\ k = m\ \forall\ m, k\in \mathbb{N}$ (since $n\in P$)

Hence, $S(n)\in P$ whenever $n\in P$. By N(v), $P = \mathbb{N}$ and so the cancellation law holds.

Q.E.D

Theorem: Multiplication

$\exists$ an unique function M: $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ with the following properties:

M(i) $M(n, 1) = n\ \forall n\in \mathbb{N}$.

M(ii) $M(n, S(m)) = A(n, M(n, m))\ \forall n, m\in \mathbb{N}$.

Let any $n\in \mathbb{N}$ be given. By the iteration theorem with $\mathbb{N}=B$, $n = b$, $\psi = A_n$,

$\exists$ an unique function M_n: $\mathbb{N}\to\mathbb{N}$ s.t $M_n(1) = n$ and $M_n\circ S(m) = A_n\circ M_n(m)$

$\forall$ m$\in\mathbb{N}$.

Define M: $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ by M(n, m) = M_n(m). M has property M(i) since M(n, 1) = M_n(1) = n $\forall$ n$\in\mathbb{N}$. M has property M(ii) since for each n$\in\mathbb{N}$,

M(n, S(m)) = M_n (S(m))
= A_n(M_n(m))
= A(n, M_n(m)
= A(n, M(n, m)) $\forall$ m$\in\mathbb{N}$.

Hence M(n, S(m)) = A(n, M(n, m)) $\forall$ n, m$\in\mathbb{N}$. If M is not a function, then $\exists$ ((n, m), l_1), ((n, m), l_2) $\in$M s.t $l_1\neq l_2$. But this imply M_n(m) = $l_1\neq l_2$ = M_n(m), contradicting M_n being a function.

Hence, $\exists$ a function M: $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ with properties M(i), M(ii).

Now, let M′ be another function with properties M(i), M(ii) and for every n$\in\mathbb{N}$, let P = {m$\in\mathbb{N}$|M(n, m) = M′(n, m)}.
Then 1$\in$P since M(n, 1) = n = M′(n, 1).
Suppose m$\in$P. Then
M(n, S(m)) = A(n, M(n, m))
= A(n, M′ (n, m)) (since m$\in$P $\Rightarrow$ M(n, m) = M′(n, m))
= M′(n, S(m))

Hence S(m)$\in$P whenever m$\in$P and by N(v), P = $\mathbb{N}$. Therefore, M(n, m) = M′(n, m) $\forall$ n, m$\in\mathbb{N}$ and so M is unique.

Q.E.D

From now on, we will denote M(n,m) as nm.

Theorem: Properties of Multiplication

M(i) n1 = n $\forall$ n$\in\mathbb{N}$.

M(ii) n(m+1) = nm + n $\forall$ n, m$\in\mathbb{N}$.

By A(v), we are allowed to make this modification to M(ii).

M(iii) n1 = 1n $\forall$ n$\in\mathbb{N}$.

Define P = {n$\in\mathbb{N}$ | n1 = 1n}.
Then 1$\in$P since (1)(1) = (1)(1). Suppose n$\in$P. Then,
S(n)1 = S(n) (by M(i))
= n1 + 1 (by M(i))
= 1n + 1 (since n$\in$P)
= 1(n+ 1) (by M(ii))
= 1S(n)

Hence S(n) $\in$P whenever n$\in$P. By N(v), P = $\mathbb{N}$ and so n1 = 1n $\forall$ n$\in\mathbb{N}$.

M(iv) (m+ 1)n= mn+ n $\forall$ n, m$\in\mathbb{N}$.

For each m$\in\mathbb{N}$, define

P = {n$\in\mathbb{N}$ | (m+1)n = mn + n}

By M(i), (m+1)1 = m + 1 = m1 + 1 so 1$\in$P. Suppose n$\in$P. Then
(m+1)S(n) = (m+1)(n+1)

$$\begin{aligned}
&= (m+1)n + (m+1) \quad \text{(by M(ii))} \\
&= mn + n + m + 1 \quad \text{(since } n\in P\text{)} \\
&= (mn+m) + (n+1) \\
&= m(n+1) + (n+1) \ \text{(by M(ii))} \\
&= mS(n) + S(n)
\end{aligned}$$

Hence $S(n)\in P$ whenever $n\in P$. By N(v), $P = \mathbb{N}$ and so $(m+1)n = mn + n$ $\forall$ $n, m\in \mathbb{N}$.

M(v) $nm = mn$ $\forall$ $n, m\in \mathbb{N}$, the commutative law of multiplication.

For each $m\in \mathbb{N}$, define

$$P = \{ n\in \mathbb{N} \mid nm = mn\}$$

Then $1\in P$ by M(iii). Suppose $n\in P$. Then,

$$\begin{aligned}
S(n)m &= (n+1)m \\
&= nm + m \quad \text{(by M(iv))} \\
&= mn + m \quad \text{(since } n\in P\text{)} \\
&= m(n+1) \quad \text{(by M(ii))} \\
&= mS(n)
\end{aligned}$$

Hence $S(n) \in P$ whenever $n\in P$. By N(v), $P = \mathbb{N}$ and so the commutative law holds.

M(vi) $m(n+k) = mn + mk$ $\forall$ $n, m, k\in \mathbb{N}$, the distributive law.

For each $m, n\in \mathbb{N}$, define

$$P = \{k\in \mathbb{N} \mid m(n+k) = mn + mk\}$$

Now,

$$\begin{aligned}
m(n+1) &= mn + m \quad \text{(by M(ii))} \\
&= mn + m1 \quad \text{(by M(i))}
\end{aligned}$$

Hence $1\in P$. Suppose $k\in P$, then

$$\begin{aligned}
m(n+S(k)) &= m((n+k) +1) \\
&= m(n+k) + m \quad \text{(by M(ii))} \\
&= mn +mk + m \quad \text{(since } k\in P\text{)} \\
&= mn + m(k+1) \quad \text{(by M(ii))} \\
&= mn + mS(k)
\end{aligned}$$

Hence $S(k)\in P$ whenever $k\in P$. By N(v), $P = \mathbb{N}$ and so the distributive law holds.

M(vii) $(nm)k = n(mk)$ $\forall$ $n, m, k\in \mathbb{N}$, the associative law of multiplication.

For each $n, m\in \mathbb{N}$, define

$$P = \{k\in \mathbb{N} \mid (nm)k = n(mk)\}$$

By M(i), $(nm)1 = nm = n(m1)$ so $1\in P$. Suppose $k\in P$.
Then

$$\begin{aligned}
(nm)S(k) &= (nm)(k+1) \\
&= (nm)k + nm \quad \text{(by M(ii))} \\
&= n(mk) + nm \quad \text{(since } k\in P\text{)} \\
&= n((mk) + m) \quad \text{(by M(vi))} \\
&= n(m(k+1)) \quad \text{(by M(ii))} \\
&= n(mS(k))
\end{aligned}$$

Hence $S(k)\in P$ whenever $k\in P$. By N(v), $P = \mathbb{N}$ and so the associative law holds.

Q.E.D

The astute reader might have noticed that we have not proved the cancellation law for multiplication. This will be proven later in the order section, where the tools developed while defining a suitable order on ℕ makes this result an easy consequence.

Theorem: Exponentiation

∃ an unique function E: ℕ×ℕ→ℕ with the following properties:

E(i) E(n, 1) = n ∀n∈ℕ.

E(ii) E(n, S(m)) = M(n, E(n, m)) ∀n, m∈ℕ.

Let any n∈ℕ be given. By the iteration theorem with ℕ=B, n = b, $\psi = M_n$,

∃ an unique function E_n: ℕ→ℕ s.t $E_n(1) = n$ and $E_n \circ S(m) = M_n \circ E_n(m)$

∀ m∈ℕ.

Define E: ℕ×ℕ→ℕ by $E(n, m) = E_n(m)$. E has property E(i) since

$E(n, 1) = E_n(1) = n$ ∀ n∈ℕ. E has property E(ii) since for each n∈ℕ,

$$
\begin{aligned}
E(n, S(m)) &= E_n(S(m)) \\
&= M_n(E_n(m)) \\
&= M(n, E_n(m)) \\
&= M(n, E(n, m)) \ \forall\ m \in \mathbb{N}.
\end{aligned}
$$

Hence E(n, S(m)) = M(n, E(n, m)) ∀ n, m∈ℕ. If E is not a function, then ∃ $((n, m), l_1)$, $((n, m), l_2)$ ∈E s.t $l_1 \neq l_2$. But this imply $E_n(m) = l_1 \neq l_2 = E_n(m)$, contradicting E_n being a function.

Hence, ∃ a function E: ℕ×ℕ→ℕ with properties E(i), E(ii).

Now, let E′ be another function with properties E(i), E(ii) and for every n∈ℕ, let

P = {m∈ℕ|E(n, m) = E′(n, m)}.

Then 1∈P since E(n, 1) = n = E′(n, 1).

Suppose m∈P. Then

$$
\begin{aligned}
E(n, S(m)) &= M(n, E(n, m),) \\
&= M(n, E'(n, m)) \quad (\text{since } m \in P \Rightarrow E(n, m) = E'(n, m)) \\
&= E'(n, S(m))
\end{aligned}
$$

Hence S(m)∈P whenever m∈P and by N(v), P = ℕ. Therefore,

E(n, m) = E′(n, m) ∀ n, m∈ℕ and so E is unique.

Q.E.D

From now on, we will denote E(n,m) as n^m.

Theorem: Properties of Exponentiation

E(i) $n^1 = n$ ∀ n∈ℕ.

E(ii) $n^{s(m)} = n^m n$ ∀ n, m∈ℕ.

By M(v), we are allowed to make this modification to E(ii)

E(iii) $1^n = 1$ ∀ n∈ℕ.

Define P = { n∈ℕ | $1^n = 1$}. Then 1∈P by E(i).

Suppose n∈P. Then,

$1^{S(n)} = 1^n 1$ (by E(ii))
$= (1)(1)$ (since $n \in P$)
$= 1$ (by M(i))

Hence $S(n) \in P$ whenever $n \in P$. By N(v), $P = \mathbb{N}$ and so $1^n = 1 \ \forall\ n \in \mathbb{N}$.

E(iv) $n^m n^k = n^{m+k} \ \forall\ n, m, k \in \mathbb{N}$.

Take any $n, m \in \mathbb{N}$ and define

$P = \{k \in \mathbb{N} \mid n^m n^k = n^{m+k}\}$

By E(i) and E(ii), $n^m n^1 = n^m n = n^{m+1}$ so $1 \in P$.

Suppose $k \in P$. Then,

$n^m n^{S(k)} = n^m n^k n$ (by E(ii))
$= n^{m+k} n$ (since $n \in P$)
$= n^{S(m+k)}$ (by E(ii))
$= n^{m+S(k)}$

Hence $S(k) \in P$ whenever $n \in P$. By N(v), $P = \mathbb{N}$ and so $n^m n^k = n^{m+k} \ \forall\ n, m, k \in \mathbb{N}$.

E(v) $(n^m)^k = n^{mk} \ \forall\ n, m, k \in \mathbb{N}$.

Take any $n, m \in \mathbb{N}$ and define

$P = \{k \in \mathbb{N} \mid (n^m)^k = n^{mk}\}$

Then $1 \in P$ since by E(i), $(n^m)^1 = n^m = n^{m1}$.

Suppose $n \in P$. Then

$(n^m)^{S(k)} = (n^m)^k (n^m)^1$ (by E(iv))
$= n^{mk} n^m$ (since $k \in P$ and by E(i))
$= n^{mk+m}$ (by E(iv))
$= n^{mS(k)}$

Hence $S(k) \in P$ whenever $k \in P$. By N(v), $P = \mathbb{N}$ and so $(n^m)^k = n^{mk} \ \forall\ n, m, k \in \mathbb{N}$.

E(vi) $(nm)^k = n^k m^k \ \forall\ n, m, k \in \mathbb{N}$.

Take any $n, m \in \mathbb{N}$ and define

$P = \{k \in \mathbb{N} \mid (nm)^k = n^k m^k\}$

Then $1 \in P$ since by E(i), $(nm)^1 = nm = n^1 m^1$.

Suppose $k \in P$. Then

$(nm)^{S(k)} = (nm)^k (nm)^1$ (by E(ii))
$= n^k m^k nm$ (since $k \in P$ and by E(i))
$= n^k\ nm^k m$
$= n^{k+1} m^{k+1}$ (by E(ii))
$= n^{S(k)} m^{S(k)}$

Hence, $S(k) \in P$ whenever $k \in P$. By N(v), $P = \mathbb{N}$ and so $(nm)^k = n^k m^k \ \forall\ n, m, k \in \mathbb{N}$.

Q.E.D

Now that we have defined 3 binary operations for ℕ, it is time to sit back and reflect on what we have just created. The astute reader will no doubt observe that all 3 definition proofs run similar, and that they rely on the function defined just before. This is no coincidence. In fact, it directly shows the true nature of each binary operation. Intuitively speaking, to add m to n is to repeatedly add 1 to n m times. Similarly, to multiply n m times is to repeatedly add n to itself m times. In a similar vein, exponentiation is just a repeating application of multiplication. We first define S(n) as n+1 as postulated by A(i). This is good but it doesn’t get us anywhere. It only gives us the addition relationship between any element and 1. We have no idea what happens if any 2 arbitrary elements get added. At first glance, we can't really expect S to do this actually, since it is after all only a $\mathbb{N}$ to $\mathbb{N}$ function. But with the aid of the iteration theorem, we can define a $\mathbb{N}\times\mathbb{N}$ to $\mathbb{N}$ function by reiterating S in a clever way! Hence, in a certain sense, we can claim that all 3 binary operations just defined are similar, i.e., their structure all arises from S. We can do without exponentiation, just that we simply has to do more multiplication. Similarly, multiplication and even addition can be forfeited. The point here is that all these binary operations have no existence of their own. They exist because S exists! Incidentally, we can appreciate how much thought has been put into constructing the five axioms. If just any one of the 5 axioms is defined inappropriately, we may never be able to construct these familiar binary operations! Before we proceed to define an order for the natural number, let us note that it is possible to devise a sort of general framework for the above 3 definition proofs. We will provide this framework in the form of a theorem, which capture the essence of the three proofs:

Theorem: General Binary Definition Machine

Suppose that for every $n\in\mathbb{N}$, $\exists$ a function F_n: $\mathbb{N}\to\mathbb{N}$. Let ϕ: $\mathbb{N}\to\mathbb{N}$ be any function. Then $\exists$ an unique function G: $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ with the following properties:

(i) $G(n, 1) = \phi(n)$ $\forall n\in\mathbb{N}$.

(ii) $G(n, S(m)) = F_n\circ G(n, m)$ $\forall n, m\in\mathbb{N}$.

Let any $n\in\mathbb{N}$ be given. By the iteration theorem with $\mathbb{N}$=B, $\phi(n)$ = b, $\psi = F_n$, $\exists$ an unique function G_n: $\mathbb{N}\to\mathbb{N}$ s.t $G_n(1) = \phi(n)$ and $G_n\circ S(m) = F_n\circ G_n(m)$ $\forall$ $m\in\mathbb{N}$.

Define G: $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ by $G(n, m) = G_n(m)$. G has property (i) since $G(n, 1) = G_n(1) = \phi(n)$ $\forall$ $n\in\mathbb{N}$. G has property (ii) since for each $n\in\mathbb{N}$,

$$\begin{aligned}G(n, S(m)) &= G_n(S(m))\\ &= F_n(G_n(m))\\ &= F_n\circ G(n, m)\ \forall\ m\in\mathbb{N}.\end{aligned}$$

Hence $G(n, S(m)) = F_n\circ G(n, m)$ $\forall$ $n, m\in\mathbb{N}$. If G is not a function, then $\exists$ $((n, m), l_1), ((n, m), l_2)\in G$ s.t $l_1\neq l_2$. But this imply $G_n(m) = l_1\neq l_2 = G_n(m)$, contradicting G_n being a function.

Hence, $\exists$ a function G: $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ with properties (i), (ii).

Now, let G′ be another function with properties (i), (ii) and for every $n\in\mathbb{N}$, let $P = \{m\in\mathbb{N}\,|\,G(n, m) = G'(n, m)\}$.

Then $1\in P$ since $G(n, 1) = \phi(n) = G'(n, 1)$.

Suppose $m\in P$. Then

$$\begin{aligned}G(n, S(m)) &= F_n\circ G(n, m)\\ &= F_n\circ G'(n, m)\ \text{(since } m\in P\Rightarrow G(n, m) = G'(n, m))\\ &= G'(n, S(m))\end{aligned}$$

Hence $S(m)\in P$ whenever $m\in P$ and by N(v), $P = \mathbb{N}$. Therefore, $G(n, m) = G'(n, m)$ $\forall$ $n, m\in\mathbb{N}$ and so G is unique.

Q.E.D

Let us now employ the above machine to recreate the 3 binary operations. The reader can then see that each binary operation is really nothing more than a repeated application of the preceding one.

Theorem:

There exist unique binary operations on $\mathbb{N}$ defined as follows:

a) Addition

A(i) $A(n, 1) = S(n)$ $\forall n \in \mathbb{N}$.

A(ii) $A(n, S(m)) = S(A(n, m))$ $\forall n, m \in \mathbb{N}$.

b) Multiplication

M(i) $M(n, 1) = n$ $\forall n \in \mathbb{N}$.

M(ii) $M(n, S(m)) = A(n, M(n, m))$ $\forall n, m \in \mathbb{N}$.

c) Exponentiation

E(i) $E(n, 1) = n$ $\forall n \in \mathbb{N}$.

E(ii) $E(n, S(m)) = M(n, E(n, m))$ $\forall n, m \in \mathbb{N}$.

a) Passing $\phi(n)=S(n)$, $F_n(m)=S(m)$ gives us the unique function $G(n, m)=A(n, m)$ such that

A(i) $A(n, 1) = S(n)$ $\forall$ $n \in \mathbb{N}$.

A(ii) $A(n, S(m)) = S(A(n, m))$ $\forall$ $n, m \in \mathbb{N}$.

For each $n \in \mathbb{N}$, we define the function A_n by

$A_n(m)=A(n, m)$ $\forall$ $m \in \mathbb{N}$

b) Passing $\phi(n)=n$, $F_n(m)= A_n(m)$ gives us the unique function $G(n, m)=M(n, m)$ such that

M(i) $M(n, 1) = n$ $\forall$ $n \in \mathbb{N}$.

M(ii) $M(n, S(m)) = A_n(M(n, m))$

$= A(n, M(n, m))$ $\forall$ $n, m \in \mathbb{N}$.

For each $n \in \mathbb{N}$, we define the function M_n by

$M_n(m)=M(n, m)$ $\forall$ $m \in \mathbb{N}$

c) Passing $\phi(n)=n$, $F_n(m)= M_n(m)$ gives us the unique function $G(n, m)=E(n, m)$ such that

E(i) $E(n, 1) = n$ $\forall$ $n \in \mathbb{N}$.

E(ii) $E(n, S(m)) = M_n(E(n, m))$

$= M(n, E(n, m))$ $\forall$ $n, m \in \mathbb{N}$.

Q.E.D

Readers would of course have noticed that this machine can produce infinite variety of binary operations on the natural numbers. We just simply feed the machine's output back to it repeatedly. Strangely enough, at the exponentiation level, properties such as commutativity and associativity fails to be preserved. We leave this as an open-ended question to the reader.

Order On ℕ

Our natural number system seems to be taking shape very nicely. We can add, multiply and even take the power of natural numbers. Is there any more concepts that we should develop? Well, any little kid can easily tell us that 2 is bigger than 1. In our current development, it seems that we can't really make this simple statement. Hence, we need to , literally, order our natural numbers. The obvious way would be the following definition:

Defn: We say that n is greater than m and we write n>m if ∃ k∈ ℕ such that n=m+k. We say that n is greater or equal to m and we write n≥ m if n>m or n=m.

Of course, we certainly do not want an ordering that places a successor of an element before it. Since S(n) is defined to be n+1, we see that our definition immediately says that ∀ n∈ ℕ,

(i) S(n) >n
(ii) S(n)>1
(iii) n>1 if n≠1 (this follows from (ii) and N(viii). Hence we also have n≥1)

Well, our definition did not contradict our fundamental notion of the 'correct order' but does it gives rise to all the desired properties? Now, our intuitive notion of the 'bigness' of a natural number parallel that of the defining properties for a total order. In fact, most concepts, such as Infimum and Suprema of a set, does not even make sense when the order employed on the set is not at least partial! Hence, we will now work towards showing that the order ≥ just defined on ℕ is indeed a total order. We will first prove the Trichotomy Law for the associated order >.

Theorem: Trichotomy Law

Let m, n∈ℕ, then one and only one of the following statements hold:
(i) m = n
(ii) m > n
(iii) m < n

We first show that at most one of the above 3 statements can be true.

Suppose (i) is true. If (ii) is true, then ∃ k∈ ℕ s.t m = n + k. Hence m = m + k, which is forbidden by A(vii). By the same reason, (iii) cannot be true also.

Now suppose (ii) is true. Then ∃ k∈ ℕ s.t m = n + k. By A(vii), (i) cannot be true. If (iii) is true, then ∃ r∈ ℕ s.t m + r = n. Then m = (m+r) + k = m + (r+k) which is forbidden by A(vii) again.

By symmetry, the truth of (iii) would result in the falsity of (i) and (ii).

Hence, at most one of the above 3 statements can be true.

We now show that at least one of the 3 statements must be true. Take any m∈ ℕ and define

P = {n∈ ℕ | at least one of (i), (ii), (iii) is true}.

Consider n = 1. If m = 1, then (i) is true. If m ≠ 1, then (ii) is true. Hence 1∈P. Suppose n∈P. Then at least one of the following is true.

(i) n = m.

Then S(n) = m + 1 and so (iii) is true for S(n).

(ii) m > n.

Then $\exists$ k$\in \mathbb{N}$ s.t m = n + k. Then m + 1 = S(n) + k. If k = 1, then by A(viii), (i) is true for S(n). If k $\neq$ 1, then $\exists$ $l \in \mathbb{N}$ s.t k = l + 1. Then m + 1 = S(n) + l + 1 and by A(viii) again, we have m = S(n) + l and so (ii) is true for S(n).

(iii)m < n.

Then $\exists$ k$\in \mathbb{N}$ s.t m + k = n. Then m + (1+k) = S(n) and so (iii) is true for S(n).

Hence, S(n)$\in$P whenever n$\in$P. By N(v), $\mathbb{N}$ = P and so the Trichotomy law holds.

Q.E.D

With the aid of the Trichotomy law, we can now easily show that $\geq$ is indeed a total order.

Theorem:

The relation $\geq$ on $\mathbb{N}$ is a partial order, which is also total.

Reflexivity is clear since n= n $\forall$ n$\in \mathbb{N}$.

Suppose m $\leq$ n and n $\leq$ m. If n $\neq$ m, we then have m < n and n < m which is forbidden by the Trichotomy law. Hence, $\leq$ is anti-symmetric.

Suppose n $\leq$ m and m $\leq$ k. If n $\leq$ k is not true, then by the Trichotomy Law, n > k. Hence, $\exists$ p$\in \mathbb{N}$ s.t n = k + p. We consider 2 cases:

(i) m = k

Then n> m which contradicts the Trichotomy law.

(ii) m < k

Then $\exists$ q$\in \mathbb{N}$ s.t m + q = k. Hence n = (m + q) + p which means m < n, contradicting the Trichotomy Law again.

Therefore, $\leq$ is transitive.

Hence, $\geq$ is a partial order.

Now take any n, m $\in \mathbb{N}$. If n=m, then n$\leq$ m by reflexivity. Otherwise, the Trichotomy law demands that n<m (hence n$\leq$ m) or n>m(hence m$\leq$ n).

Hence, $\geq$ is also a total order.

Q.E.D

Theorem: Properties of order

We will now derive some elementary properties of order under the various binary operations. For all n, m, k, r$\in \mathbb{N}$, we have

(1) n < m and m < k $\Rightarrow$ n < k

This is a simple consequence of $\leq$ being transitive.

(2) n < n is never true.

This follows directly from A(vii)

Addition

(3) If n $\neq$ m, then one and only one of the equation x + m = n and x + n = m has a solution in $\mathbb{N}$ and this solution is unique.

By the Trichotomy law, the first part of the assertion is trivially true. We need only to show that the solution is unique. Let us assume that the equation x + p = q has a solution in $\mathbb{N}$ and let x_1, $x_2 \in \mathbb{N}$ be any 2 solutions. Then x_1+ p = q and x_2+ p = q so that x_1+ (p+q) = x_2+ (p+q). By A(viii), $x_1 = x_2$ and so the solution is unique.

(4) n + m > n

Since (n+m) = (n) + m, the assertion is trivially true.

(5) m > n ⇔ m + k > n + k

If m > n, then ∃ p∈ ℕ s.t m = n + p. Hence (m+k) = (n+k) + p and so m + k > n + k..

Conversely, if m + k > n + k, then ∃ p∈ ℕ s.t m + k = n + k + p and by A(viii), m = n + p and so m > n.

(6) m > n and k > r ⇒ m + k > n + r.

∃ p, q∈ ℕ s.t m = n + p and k = r + q. Hence, m + k = (n+r) + (p+q) and so m + k > n + r.

(7) m < n + 1 iff m ≤ n

Let m < n + 1 and m > n. Then ∃ p, q∈ ℕ s.t m + p = n + 1 and m = n + q. Then n + 1 + m = m + p + n + q and by A(viii), 1 = p + q, i.e. 1 > p. But 1 ≤ p which contradicts the Trichotomy law. Hence, by Trichotomy law again, m < n + 1 ⇒ m ≤ n. Conversely, if m ≤ n, then m + 1 ≤ n + 1 by (5). Now, m < m + 1. If m + 1 = n + 1, we have m < n + 1. Otherwise, i.e. if m + 1 < n + 1, then by (1), we still have m < n + 1. Hence, m < n + 1 ⇔ m ≤ n.

(8)There does not exist m∈ ℕ s.t n < m < n + 1.

Let such an m exist. By (7), we then have n < m ≤ n. This contradict the Trichotomy law and so m cannot exist.

Multiplication

(9) n < m iff nr < mr.

If n < m, then ∃ p∈ ℕ s.t n + p = m. Hence nr + pr = mr by M(vi) and so nr < mr. Conversely, if nr < mr, then if

(i) m = n.

We then have mr = nr which contradict the Trichotomy law.

(ii) n > m.

Then ∃ p∈ ℕ s.t n = m + p. Hence nr = mr + pr so that nr > mr. This again contradicts the Trichotomy law.

Hence nr < mr ⇒ n < m by the Trichotomy law. Therefore n< m ⇔ nr< mr.

(10)(or M(viii)) nm = nk ⇒ m = k, cancellation law for multiplication.

If nm = nk but m ≠ k, then either m > k or m < k. In both cases, (9) imply that nm ≠ nk which gives a contradiction. Hence, nm = nk ⇒ m = k.

(11) n < m and k < r ⇒ nk < mr.

By (9), we have nk < mk and mk < mr. Then (1) demands nk < mr.

(12) nm ≥ n

If m=1, then equality holds trivially. Otherwise, we can write m=1+k for some k∈ ℕ. The statement reduces to n+nk ≥ n which is true by (4).

Exponentiation

(13) n < m iff n^k< m^k

For each n, m∈ ℕ, define

P = {k∈ ℕ | n < m iff $n^k < m^k$}

Obviously, 1∈P. Suppose k∈P.

If n < m, then $n^k < m^k$. By (11), $n^k n < m^k m$ and so n < m ⇒ $n^{k+1} < m^{k+1}$. Conversely, if $n^{k+1} < m^{k+1}$, then if

(i) n = m.

By (9), we must have $n^k < m^k$, which result in $n < m$ since $k \in P$ and hence contradict the Trichotomy law.

(ii) $n > m$.

By (11), we have

$mn^{k+1} < nm^{k+1}$

$\Rightarrow n^k < m^k$ by (9)

$\Rightarrow n < m$ (since $k \in P$)

This is again not possible since it contradicts the trichotomy law.

Hence, $S(k) \in P$ whenever $k \in P$. By N(v), $P = \mathbb{N}$ and so $n < m$ iff $n^k < m^k$.

By letting $n = 1$, we can observe that $1<m$ iff $1 < m^k$.

(14) $(n+1)^m \geq 1 + nm$

Let $P = \{m \in \mathbb{N} \mid (n+1)^m \geq 1 + nm\}$.

When $m = 1$, equality holds and so $1 \in P$. Suppose $m \in P$. Suppose also that $(n+1)^{m+1} < 1 + n(m+1)$. Then $(n+1)^m n + (n+1)^m < 1 + nm + n$. We consider 2 cases:

(i) $(n+1)^m = 1 + nm$

By (5), we have

$(n+1)^m n < n$

$\Rightarrow (n+1)^m < 1$ (by (9))

Hence, this is not possible.

(ii) $(n+1)^m > 1 + nm$

Then $(n+1)^m + n > 1 + nm + n$. By (1),

$(n+1)^m + n > (n+1)^m n + (n+1)^m$

$\Rightarrow n > (n+1)^m n$ (by (5))

$\Rightarrow 1 > (n+1)^m$ (by (9))

Similarly, this leads to a contradiction.

Hence, $(n+1)^{m+1} < 1 + n(m+1)$ is not possible and so by the trichotomy law, $S(m) \in P$ whenever $m \in P$. By N(v), $P = \mathbb{N}$ and so $(n+1)^m > 1 + nm$.

(15) $m^k \geq k + 1$, $m \neq 1$

Since $m \neq 1$, then by N(viii), $\exists\, n \in \mathbb{N}$ s.t $m = n + 1$. Then

$m^k = (n+1)^k$

$\geq 1 + nk$ (by (14))

$\geq 1 + k$ (by (9), (5) and since $n \geq 1$)

Hence, $m^k \geq 1 + k$, $m \neq 1$.

Q.E.D

Intuitively, we all know that for any natural number, we can make the product as ‘big as we please’ by multiplying it with another suitable natural number. This seem to be obviously trivial but it is in fact a very important fundamental property of $\mathbb{N}$, the absence of which would render us helpless in proving many things. It is also a fundamental property of the real number system which we are eventually going to construct. As it is so important, we will prove it here now. For readers with a certain maturity in math, you have guessed it! It is the famous Archimedean Property!

Theorem: Archimedean Property

Let $m, n \in \mathbb{N}$. Then $\exists\, k \in \mathbb{N}$ s.t $mk > n$.

For any $m, n \in \mathbb{N}$, take $k = S(n)$. Then

$mS(n) = mn + m$
$> mn$ (by (4))
$\geq n$ (by (9) and since $m \geq 1$)
Hence, the Archimedeon property holds.

Q.E.D

We also have an exponentiation version, but note that that is not a common feature to the rest of the number system which we are eventually going to create. We prove it here now:

Theorem: Archimedean Property (exponentiation version)

Let m, n∈ℕ, m ≠ 1. Then ∃ k∈ℕ s.t $m^k > n$.

For any m, n∈ℕ, m ≠ 1, take k = n. Then
$m^n \geq n + 1$ (by (15))
$> n$
Hence, the Archimedean property (for exponentiation) holds.

Q.E.D

Mathematical Induction

Usually, there are statements that are true for all n∈ℕ except perhaps for a finite number of cases. In such cases, we cannot use N(v) directly, since N(v) explicitly demand that the case n = 1 must be true. Notice how awkward our definition of P is, in N(viii), when all we want to achieve is to exclude the case n = 1. What happens when we want to exclude more cases? Would not our proof become unnecessarily cumbersome?

Here, we will see one of the benefits of ordering our natural numbers. We can now show that it is possible to start our induction from any arbitrary k∈ℕ by using our newly defined terminology. We give a formal proof below.

Theorem: Modified principle of induction

Let A ⊆ℕ be s.t
(a) k∈A
(b) S(n)∈A whenever n∈A ∀n ≥ k
Then n∈A ∀n ≥ k.

Define

P = {n∈ℕ | n < k or n∈A}

Now, if k = 1, then the statement is just N(v) and hence there is nothing to prove. We assume then that k ≠ 1. Now, 1∈P since 1< k. Suppose n∈P. Then either

(i) n < k

Hence we must have S(n) ≤ k. If S(n) < k, then S(n)∈P by definition. Otherwise, S(n) = k and we still have S(n)∈P since k∈A by (a).

(ii) n∈A

We can always assume n ≥ k. Otherwise, we simply appeal to (i). Hence, it is obvious from (b) that S(n)∈A and so S(n)∈P.

Hence S(n)∈P whenever n∈P. By N(v), P = ℕ. Now take any n∈ℕ, n ≥ k. Then n∈P and by the defining property of P, the Trichotomy law forces n∈A and so our claim is true.

Q.E.D

We also mention the general principle of induction and show that it is actually equivalent to N(v).

Theorem: General principle of induction

Let A⊆ℕ be s.t

(a) 1∈A

(b) S(n)∈A whenever {k∈ℕ | k≤ n} ⊆A

Then A=ℕ

The above statement known as the General principle of induction is equivalent to N(v).

Assume the general principle of induction is true. Let A⊆ ℕ s.t

(c) 1∈A

(d) S(n)∈A whenever n∈A

Then

(a) 1∈A (by (c))

(b) {k∈ℕ | k≤ n} ⊆ A⇒ n∈A

⇒ S(n)∈A (by (d))

Hence, by general principle of induction, A= ℕ and so N(v) is true.

Conversely, assume that N(v) is true. Let A⊆ ℕ s.t

(a) 1∈A

(b) S(n) ∈A whenever {k∈ℕ | k≤ n} ⊆ A

Define

P={ n∈ℕ |{k∈ℕ | k≤ n} ⊆ A}

First, observe that P⊆ A since n∈ P⇒ {k∈ℕ | k≤ n} ⊆ A⇒ n∈A. Now, {k∈ℕ | k≤ 1}= {1}⊆ A (by (a)) and so 1∈ P. Suppose n∈ P. Then by (b), S(n) ∈ A and so {k∈ℕ | k≤ S(n)} ⊆ A. Note that this is true since {k∈ℕ | k≤ S(n)}= {k∈ℕ | k≤ n}∪ {S(n)}. Hence, S(n)∈ P whenever n∈ P. By N(v), P= ℕ. Since ℕ =P⊆ A⊆ ℕ, it follows that A= ℕ and so the general principle of induction is true.

Hence, N(v) and the general principle of induction is equivalent.

Q.E.D

The Well Orderedness Of ℕ

We proved early in this chapter that ℕ is actually an infinite set. Although this is rather a useful property, it does not make ℕ stand out from the rest. After all, the integers, rationals, and reals are also all infinite sets. If we imagine our standard number line, we can see one significant difference between ℕ and the rest. The integers, rationals and the reals all stretch towards both side of the number line indefinitely. In contrast, ℕ only stretches to the right, that is, it has a 'starting point' 1. Of course, we can conceptually say that the integers, rationals and the reals also have a starting point 'minus infinity' but the crux is that technically, 'minus infinity' is not an element of the integers, rationals or the reals. Even in an intuitive sense, 'minus infinity' is just a way of speaking and does not really constitute a physical point. This special property of ℕ translate roughly to the concept of well-ordered set. Before we attempt to show that ℕ is well-ordered, we will first prove that a certain kind of subset of ℕ, the intervals, is finite.

<u>Theorem: Pigeonhole Principle</u>

For every n∈ℕ, the set [1, n]:={m∈ℕ | 1 ≤ m ≤ n} is a finite set.

Define

P = {n∈ℕ | [1, n] is finite}.

Clearly, ∃ one and only one one-one function F: {1}→ {1} and it is obviously onto. Hence, 1∈P. Suppose n∈P. We first note that, since there is no natural number strictly between n and S(n), it is true that [1, S(n)] = [1, n]∪{S(n)}. Take any one-one function F: [1, S(n)]→ [1, S(n)]. We consider 2 cases.

(i) F[1, n] ⊆ [1, n]

Hence, we can define F′: [1, n]→ [1, n] by

F′(m) = F(m) ∀ m∈[1, n].

Then F′ is onto [1, n] since F′ is one-one and n∈P. Hence, we need only to show that S(n)∈F[1, S(n)]. We claim F(S(n)) = S(n) for if this is not so, then F(S(n))∈[1, n] and so ∃ k∈[1, n] s.t F(S(n)) = F(k). But k ≠ S(n), contradicting the one-one nature of F. Hence F is onto [1, S(n)].

(ii) F[1, n] ⊈ [1, n]

Hence, ∃ k∈[1, n] s.t F(k) = S(n). Since F is one-one, we are assured that F(m) ≠ S(n) if m ≠ k. In particular, F(S(n)) ≠ S(n). We then define F′: [1, n]→ [1, n] by

F′(m) = F(m) if m∈[1, n], m ≠ k.

F′(k) = F(S(n))

Observe that F′ is still one-one since F′(m) ≠ F(S(n)) ∀ m∈[1, n] / {k}. Hence, since n∈P, F′ is onto [1, n]. Hence, F(k) = S(n) and for every m∈[1, n], ∃ *l*∈[1, S(n)] / {k} s.t F(*l*) = m and so F is onto [1, S(n)].

Hence, S(n)∈P whenever n∈P. By N(v), P = ℕ and so the pigeonhole principle holds.

Q.E.D

The next theorem is our last theorem on ℕ and it tells us the relationship between bounded sets and infinite sets in ℕ. In particular, it allows us to conclude that ℕ is well-ordered, a property that will prove to be quite useful in later developments.

Theorem:

Let T be a non-empty subset of ℕ. Then the following holds:

(i) T is always bounded below. Furthermore, InfT exists and it is in T. Also,

InfT = 1 iff $1\in T$.
(ii) If T is bounded above, then SupT exists and is in T
(iii) T is infinite iff T is not bounded above.

(i) Let $L = \{n\in \mathbb{N} \mid n \leq t \ \forall \ t\in T\}$. Obviously, $1\in L$ and so T is always bounded below. We first observe that if $t\in T$, then $S(t)\notin L$ since $S(t) > t$. Hence, we conclude $L \neq \mathbb{N}$. Hence, $\exists \ l_0\in L$ s.t $S(l_0)\notin L$ else by N(v), $L = \mathbb{N}$.

Now, suppose $\exists \ l_1\in L$ s.t $l_1 > l_0$. Since there is no natural number strictly between a natural number and its successor, we must have $l_1 \geq S(l_0)$. But $S(l_0)\notin L$ so $\exists \ t_0\in T$ s.t $S(l_0) > t_0$. Hence $l_1 > t_0$ which contradict $l_1\in L$. Hence l_0 = InfT and so InfT exist.

If $l_0\notin T$, we then have $l_0 < t \ \forall \ t\in T$. This is absurd since in particular, we would then have $l_0 < t_0 < S(l_0)$, which contradict the fact that there is no natural number strictly between a natural number and its successor. Hence InfT$\in$T.

If InfT = 1, then we have just proved above that $1\in T$. Conversely, if $1\in T$, then 1 is the only lower bound and hence must be InfT.

(ii) Let $U = \{n\in \mathbb{N} \mid n \geq t \ \forall \ t\in T\}$. Then U is a non-empty subset of $\mathbb{N}$ and by (i), InfU exists and is in U. Since InfU$\in$U and InfU $\leq$ n $\forall$ n$\in$U, it follows that infU = SupT and so SupT exists. Suppose SupT$\notin$T. Then t < SupT $\forall$ t$\in$T. Since T is non-empty, SupT $\neq$ 1. Hence, $\exists$ m$\in \mathbb{N}$ s.t S(m) = SupT. Since there is no natural number strictly between a natural number and its successor, $t \leq m \ \forall \ t\in T$ and so $m\in U$. But m < S(m), contradicting SupT being the suprema of T. Hence SupT$\in$T.

(iii) Suppose T is not bounded above. For any $n\in T$, let $C_n = \{m\in T \mid m > n\}$. Then C_n is non-empty since T is not bounded above. By (i), $\text{Inf}C_n$ exists and is in C_n . Since $\text{Inf}C_n\in C_n$, $\text{Inf}C_n \geq n + 1$ and also, $\text{Inf}C_n\in T$. Define f: T$\rightarrow$ T by
$f(n) = \text{Inf}C_n \ \forall \ n\in T$.

Let $\text{Inf}C_n = \text{Inf}C_{n'}$. If $n < n'$, then $n'\in C_n$ and so $\text{Inf}C_n \leq n' < n' + 1 \leq \text{Inf}C_{n'}$ which is a contradiction. Similarly $n > n'$ is impossible and so $n = n'$. Hence f is one-one. Also, $\text{InfT} \leq n < n + 1 \leq \text{Inf}C_n \ \forall \ n\in T$. Hence, InfT$\notin$ f(T) but by (i), InfT$\in$T and so T $\neq$f(T). Hence f is onto some proper subset of T and so it is infinite.

Now, suppose T is bounded above. Hence, SupT exists by (ii). Then T $\subseteq$ [1, SupT]. Since [1, SupT] is finite, T must also be finite.

Hence, T is infinite iff T is not bounded above.

Q.E.D

As statement(i) of the theorem indicate,$\mathbb{N}$ is a **well-ordered** set. We mentioned earlier that this is mainly due to $\mathbb{N}$ having a 'starting point'. If we make a careful analysis of the proof of the theorem, we will see that it relies heavily on the fact that there is no natural number strictly between a natural number and its successor, as proved in (8) of order properties. This is the intuitive concept of discreteness and is also a major factor why $\mathbb{N}$ is well- ordered. As we will see later, $\mathbb{Z}$ is also discrete but it fails to be well-ordered since it does not have a 'starting point'. Note that statement(i) and (ii) of the theorem also tells us that $\mathbb{N}$ is **order complete**. The concept of order completeness will figure prominently in the later part of our construction, and is in fact the major motivation behind the creation of the irrational numbers! Hence, we shall first delay our discussion on order completeness. We end this chapter with a discussion on why ℕ is not satisfactory by itself. This will motivate the creation of the integer system ℤ.

The Inadequacy Of ℕ

This section is not meant to denounce ℕ as a faulty or imperfect system. As a counting system, ℕ is wonderful and perfect. But as man progresses through the ages, he needs a system that can do more than counting. In particular, as his herd of sheep is being decimated steadily by wolves, he needs a method of subtraction so that he can keep count of the number of sheep lost. Now, for this purpose, there is no need to postulate an integer system. Children in school are taught subtraction in ℕ, and they do not need the concept of a negative number. The teachers are always careful to give them values that remain in the domain of ℕ.A primitive shepherd is just like our modern child. The wolves cannot eat more sheep than he initially has, so he never has to bother about negative numbers.

Why do we then need an integer system? Can we not just create a binary subtraction for ℕ? Well, as man starts to dabble in commerce, he came up with the concept of debts. Now, it is possible to 'take away' more than one once have and so we cannot possibly always uses the elements of ℕ to represent our current financial status. In fact, this statement is made precise in (3) in order properties, which essentially say in a technical way that ℕ do not have enough elements to do self-contained subtraction. Hence, we need an integer system, a system which contains our normal natural system and furthermore, has 'new elements' that can represent a poor debtor's status. In fact, we are actually really going to create a binary subtraction for ℕ, just that as binary operation must be closed, we keep adding elements to ℕ until we satisfy this criteria! The resulting system is the integer system, which turns out to have some rather interesting properties of its own.

End of Chapter 1

CHAPTER 2: THE INTEGER SYSTEM

Introduction

There are many ways to visualize the integers, but the most natural way would be to think of them in terms of the natural numbers. All statements regarding negative integers can always be rephrased so that we only quote natural numbers. For example, a car that is moving at –20 km/hr is doing nothing more than travelling backward at 20km/hr. A person whose current financial status is -\$200 can always tell people he used to have \$300 but cannot resist buying a gold chain for \$500. Even for positive integers, we can always be fanciful and say that 2 is the difference of 7 and 5, or 8 and 6 or 100 and 98 and so on and so forth.

In this chapter, we will use this basic intuitive idea to create the integer system from the natural numbers which we have already constructed. The next section gives a precise formulation of a particular system that will eventually prove to be an integer system.

The Net Difference System

We consider here ordered pairs of natural numbers and try to classify them according to the difference between the first value and the latter. Our system, called the net difference system will then consist of elements whose nature are actually a sort of collection of related pairs. If it helps one's intuition, we can always think of a particular element of this system, which we will call say [2] , as a house in which there lived infinite number of pairs such as (7,5), (5,3), (10,8) etc. The house [-3] will have residents such as (2,5), (9,12) and so on. If the idea is clear, then the following definition should make sense:

Defn: For (n, m), (r, s)$\in$ $\mathbb{N}\times\mathbb{N}$, we say (n, m) is equivalent to (r, s) and write it as (n, m)~(r, s) if n + s = m + r.

In fact, we are trying to define an equivalence relation on $\mathbb{N}\times\mathbb{N}$ so that each class represent a particular integer. That our relation is actually an equivalence relation is very important, since we certainly want to make sure that each pair lives in one and only one house. We prove it here now.

Theorem:

The relation ~ is an equivalence relation on $\mathbb{N}\times\mathbb{N}$.

Since n + m = m + n, we easily have (n, m)~(n, m).
Hence ~ is reflexive.
Since n + s = m + r $\Rightarrow$ r + m = s + n, we have (n, m)~(r, s) $\Rightarrow$ (r, s)~(n, m).
Hence, ~ is symmetric.
Let (n, m)~(r, s) and (r, s)~(k, l). Then we have n + s = m + r and r + l = s + k.
Hence,

$$(n + s) + (r + l)= (m + r) + (s + k)$$

$$\Rightarrow \quad n + l = m + k$$

Thus, (n, m)~(r, s) and (r, s)~(k, l) $\Rightarrow$ (n, m)~(k, l)

Hence ~ is transitive.

Hence ~ is an equivalence relation on $\mathbb{N}\times\mathbb{N}$.

Q.E.D

We will denote the set $\mathbb{N}\times\mathbb{N}/\sim$ in our Net Difference System by $\mathbb{Z}$. An element [(n,m)] in $\mathbb{Z}$ will now be simply written as [n, m]. Now, we have only produced the elements in $\mathbb{Z}$. A bunch of elements can hardly be called a system. We still need to define appropriate binary operations and an order on it just as we did for $\mathbb{N}$. Before we do so, let us note the following fundamental relation between elements in $\mathbb{Z}$:

Lemma:

[m, n] = [m+k, n+k] $\forall$ n, m, k $\in \mathbb{N}$

$[m, n] = [m+k, n+k] \Leftrightarrow m + (n+k) = n + (m+k)$

$\Leftrightarrow m + n + k = m + n + k$ (a tautology!)

Q.E.D

Binary operation on $\mathbb{Z}$

In this section, we will define addition and multiplication on $\mathbb{Z}$. If the machinery of the Net Difference System is understood properly, then the reader should have no problem coming up with the same definitions with some elementary arithmetic.

Theorem: Addition on $\mathbb{Z}$

$\exists$ a well-defined binary operation $\oplus$ on $\mathbb{Z}$ given by

[m, n] $\oplus$ [k, r] = [m+k, n+r] $\forall$ n, m, k, r $\in \mathbb{N}$.

To show that $\oplus$ is well-defined, we need to show that for any $([m, n], [k, r]) \in \mathbb{Z}\times\mathbb{Z}$, it has one and only one image under $\oplus$. Hence, let

$[m, n] = [m', n']$ and $[k, r] = [k', r']$. Then $[m, n] \oplus [k, r] = [m+k, n+r]$ and

$[m', n'] \oplus [k', r'] = [m'+k', n'+r']$. Now,

$[m, n] = [m', n'] \Rightarrow m + n' = n + m'$

$[k, r] = [k', r'] \Rightarrow k + r' = r + k'$

Hence,

$(m+n') + (k+r') = (n+m') + (r+k')$

$\Rightarrow (m+k) + (n'+r') = (m'+k') + (n+r)$

$\Rightarrow [m+k, n+r] = [n'+r', m'+k']$

Hence, $\oplus$ is well-defined.

Q.E.D

Theorem: Properties of addition on $\mathbb{Z}$

$\forall$ [m, n], [k, r], [p, q] $\in \mathbb{Z}$, we have:

$A_{\mathbb{Z}}$(i) [m, n] $\oplus$ [k, r] = [k, r] $\oplus$ [m, n]

$[m, n] \oplus [k, r] = [m + k, n + r]$

$$= [k + m, r + n]$$
$$= [k, r] \oplus [m, n]$$

$A_{\mathbb{Z}}$(ii) $([m, n]\oplus[k, r]) \oplus [p, q] = [m, n] \oplus ([k, r]\oplus[p, q])$

$$\begin{aligned}([m, n]\oplus[k, r]) \oplus [p, q] &= [m + k, n + r] \oplus [p, q]\\ &= [(m+k) + p, (n+r) + q]\\ &= [m + (k+p), n + (r+q)]\\ &= [m, n] \oplus [k + p, r + q]\\ &= [m, n] \oplus ([k, r]\oplus[p, q])\end{aligned}$$

$A_{\mathbb{Z}}$(iii) The identity element exist for $\oplus$ and it is given by $[1, 1]$.

$$\begin{aligned}[m, n] \oplus [1, 1] &= [m + 1, n + 1]\\ &= [m, n]\\ &= [1, 1] \oplus [m, n] \quad (\text{by } A_{\mathbb{Z}}(i))\end{aligned}$$

$A_{\mathbb{Z}}$(iv) For each $[m, n]\in \mathbb{Z}$, its $\oplus$-inverse exist and is given by $[n, m]$.

$$\begin{aligned}[m, n] \oplus [n, m] &= [m + n, n + m]\\ &= [m + n + 1, m + n + 1]\\ &= [1, 1]\\ &= [n, m] \oplus [m, n] \ (\text{by } A_{\mathbb{Z}}(i))\end{aligned}$$

Q.E.D

As the reader may have noticed, we have in fact shown that $(\mathbb{Z}, \oplus)$ is a commutative group.

<u>Theorem: Multiplication on $\mathbb{Z}$</u>

$\exists$ a well-defined operation $\odot$ on $\mathbb{Z}$ given by

$[m, n]\odot[k, r] = [mk + nr, nk + mr]$ $\forall n, m, k, r\in \mathbb{N}$.

Let $[m, n] = [m', n']$ and $[k, r] = [k', r']$.

Then

$[m, n] = [m', n'] \Rightarrow m + n' = n + m'$

$[k, r] = [k', r'] \Rightarrow k + r' = r + k'$

Now,

$$[m, n]\odot[k, r] = [m', n']\odot[k', r']$$
$$\Leftrightarrow [mk + nr, nk + mr] = [m'k'+ n'r', n'k' + m'r']$$
$$\Leftrightarrow (mk + nr) + (n'k' + m'r') = (nk + mr) + (m'k'+ n'r')$$
$$\Leftrightarrow mk+ nr + n'k' + m'r' + (n'k + m'r+nr'+mk')=nk+mr+m'k'+n'r'+(n'k+m'r +nr'+mk')$$
$$\Leftrightarrow (m +n')k+(m+n')k'+(m'+n)r'+(m'+n)r=n(r' + k) + m(r + k') + m'(k' + r) + n'(r' + k)$$
$$\Leftrightarrow (m + n')(k + k' + r' + r) = (r + k')(n + m + m' + n') \quad (\text{since } m+n'=n+m', k+r'=r+ k')$$
$$\Leftrightarrow (m + n')((r + k') + (k + r')) = (r + k')((m + n') + (n + m'))$$
$$\Leftrightarrow (m + n')(2)(r + k') = (r + k')(2)(m + n')$$
$$\Leftrightarrow 2(m + n')(r + k') = 2(m + n')(r + k') \qquad (\text{a tautology!})$$

Hence, $\odot$ is well defined.

Q.E.D

<u>Properties of multiplication on $\mathbb{Z}$</u>

$\forall l, s, m, n, k, r\in \mathbb{N}$, we have

$M_{\mathbb{Z}}$(i) $[m, n]\odot[k, r] = [k, r]\odot[m, n]$

$$\begin{aligned}[m, n]\odot[k, r] &= [mk + nr, nk + mr]\\ &= [km + rn, rm + kn]\\ &= [k, r]\odot[m, n]\end{aligned}$$

$M_{\mathbb{Z}}$(ii) $([m, n]\odot[k, r])\odot[l, s] = [m, n]\odot([k, r]\odot[l, s])$

$$\begin{aligned}([m, n]\odot[k, r])\odot[l, s] &= [mk + nr, nk + mr]\odot[l, s]\\ &= [(mk+ nr)l + (nk + mr)s, (nk + mr)l + (mk + nr)s]\\ &= [mkl + nrl + nks + mrs, nkl + mrl + mks + nrs]\\ &= [(mkl + mrs) + (nrl + nks), (nkl + nrs) + (mrl + mks)]\\ &= [m(kl + rs) + n(rl + ks), n(kl + rs) + m(rl + ks)]\\ &= [m, n]\odot([k, r]\odot[l, s])\end{aligned}$$

$M_{\mathbb{Z}}$(iii) The identity element exist for $\odot$ and is given by [2, 1]

$$\begin{aligned}[m, n]\odot[2, 1] &= [m2 + n1, n2 + m1]\\ &= [m + m + n, n + n + m]\\ &= [m + (m + n), n + (m + n)]\\ &= [m, n]\\ &= [2, 1]\odot[m, n] \text{ (by } M_{\mathbb{Z}}\text{(i))}\end{aligned}$$

$M_{\mathbb{Z}}$(iv) $[m, n]\odot([k, r]\oplus[l, s]) = ([m, n]\odot[k, r])\oplus([m, n]\odot[l, s])$

$$\begin{aligned}[m, n]\odot([k, r]\oplus[l, s]) &= [m, n]\odot[k + l, r + s]\\ &= [m(k + l) + n(r + s), n(k + l) + m(r + s)]\end{aligned}$$

$$\begin{aligned}([m, n]\odot[k, r])\oplus([m, n]\odot[l, s]) &= [mk + nr, nk + mr]\oplus[ml + ns, nl + ms]\\ &= [(mk + nr) + (ml + ns), (nk+mr) + (nl + ms)]\\ &= [m(k + l) + n(r + s), n(k + l) + m(r + s)]\\ &= [m, n]\odot([k, r]\oplus[l, s])\end{aligned}$$

$M_{\mathbb{Z}}$(v) $[m, n]\odot[k, r] = [1, 1] \Rightarrow [m, n] = [1, 1]$ or $[k, r] = [1, 1]$

Now,

$[m, n]\odot[k, r] = [1, 1]$

$\Rightarrow [mk + nr, nk + mr] = [1, 1]$

$\Rightarrow (mk + nr) + 1 = (nk + mr) + 1$

$\Rightarrow mk + nr = nk + mr$

Suppose $[m, n] \neq [1, 1]$. Then $m \neq n$. We consider 2 cases.

(i) $m > n$

$\exists\, l\in \mathbb{N}$ s.t $m = n + l$. Hence

$mk + nr = nk + mr$

$\Rightarrow (n + l)k + nr = nk + (n + l)r$

$\Rightarrow nk + lk + nr = nk + nr + lr$

$\Rightarrow lk = lr$

$\Rightarrow k = r$

$\Rightarrow [k, r] = [1, 1]$

(ii) $m < n$

By symmetry, we still have

$mk + nr = nk + mr \Rightarrow k = r \Rightarrow [k, r] = [1, 1]$

Hence,

$[m, n]\odot[k, r] = [1, 1] \Rightarrow [k, r] = [1, 1]$ if $[m, n] \neq [1, 1]$

Q.E.D

Hence, we have shown that $(\mathbb{Z},\oplus,\odot)$ is an integral domain. This is an especially useful result, since it allows us to make use of general algebra rules that are proved for integral domain. In fact, we are putting the cart before the horse. The concept of an integral domain was inspired through a fundamental intuition of the integers, and so this result should really come as no surprise!

Order On $\mathbb{Z}$

After defining the two familiar binary operations on $\mathbb{Z}$, the next natural thing to do is to order the elements in $\mathbb{Z}$. Our aim here is to define an order that will make $\mathbb{Z}$ an ordered integral domain. This means we first have to postulate a subset of $\mathbb{Z}$ that serves as our set of 'positive integers'. Intuitively, this set should turn out eventually to resemble $\mathbb{N}$. Hence, we employ the following suggestive notation:

Defn: We define the subset $\mathbb{N}_{\mathbb{Z}}$ of $\mathbb{Z}$ by $\mathbb{N}_{\mathbb{Z}}:= \{[n+1, 1]\in\mathbb{Z} \mid n\in\mathbb{N}\}$

The following theorem tells us that $\mathbb{N}_{\mathbb{Z}}$ appears to be indeed a very good model of $\mathbb{N}$. It will come in useful later when we try to show the existence of a general integer system. We prove it here now since it gives us certain properties of $\mathbb{N}_{\mathbb{Z}}$ that is useful in our quest to define an appropriate order.

Theorem:

For the set $\mathbb{N}_{\mathbb{Z}}$, the following holds:

(i) $(\mathbb{N}_{\mathbb{Z}}, \oplus)$ is a sub-semigroup of $(\mathbb{Z}, \oplus)$

(ii) $(\mathbb{N}_{\mathbb{Z}}, \odot)$ is a sub-semigroup of $(\mathbb{Z}, \odot)$

(iii) $(\mathbb{N}_{\mathbb{Z}}, \oplus)$ is isomorphic to $(\mathbb{N}, +)$ and $(\mathbb{N}_{\mathbb{Z}}, \odot)$ is isomorphic to $(\mathbb{N}, .)$ as semi-groups under the same isomorphism.

(iv) For every $x\in\mathbb{Z}$, $\exists y, z\in\mathbb{N}_{\mathbb{Z}}$ s.t $x = y \oplus (-z)$.

Take any $[n+1, 1], [m+1, 1]\in\mathbb{N}_{\mathbb{Z}}$.

(i) $[n+1, 1] \oplus [m+1, 1] = [n+m+1+1, 1+1]$

$= [(n+m)+1, 1]$ $(\in\mathbb{N}_{\mathbb{Z}})$

Since $\mathbb{N}_{\mathbb{Z}}$ is closed under $\oplus$, $(\mathbb{N}_{\mathbb{Z}}, \oplus)$ is a sub-semigroup of $(\mathbb{Z}, \oplus)$.

(ii) $[n+1, 1] \odot [m+1, 1] = [(n+1)(m+1) + (1)(1), (1)(m+1) + (n+1)(1)]$

$= [nm + n + m + 1 +1, m + 1 + n + 1]$

$= [nm + 1, 1]$ $(\in\mathbb{N}_{\mathbb{Z}})$

Since $\mathbb{N}_{\mathbb{Z}}$ is closed under $\odot$, $(\mathbb{N}_{\mathbb{Z}},\odot)$ is a sub-semigroup of $(\mathbb{Z},\odot)$.

(iii) Define ϕ: $\mathbb{N}_{\mathbb{Z}}\rightarrow \mathbb{N}$ by

$\phi([n+1, 1]) = n$

We first show that ϕ is a well-defined function. Hence let

$[n'+1, 1] = [n+1, 1]$, i.e.

$(n'+1, 1) \sim (n+1, 1) \Leftrightarrow (n'+1) + 1 = 1 + (n+1)$

$$\Leftrightarrow n' = n$$

i.e. $[n+1, 1] = [n'+1, 1] \Rightarrow \phi([n+1, 1]) = \phi([n'+1, 1])$ and so ϕ is well-defined.

Now,

$$\phi([n+1, 1]) = \phi([n'+1, 1]) \Rightarrow n = n'$$
$$\Rightarrow [n+1, 1] = [n'+1, 1]$$

Hence, ϕ is one-one.

For any $n\in \mathbb{N}$, take $[n+1, 1]\in \mathbb{N}_{\mathbb{Z}}$ so that $\phi([n+1, 1]) = n$ and so ϕ is onto.

Now, take any $[n+1, 1], [m+1, 1]\in \mathbb{N}_{\mathbb{Z}}$.

$$\begin{aligned}\phi([n+1, 1] \oplus [m+1, 1]) &= \phi([(n+1) + (m+1), 1+1]) \\ &= \phi([(n+m) + 1, 1]) \\ &= n + m \\ &= \phi([n+1, 1]) + \phi([m+1, 1])\end{aligned}$$

Hence, $(\mathbb{N}_{\mathbb{Z}}, \oplus) \simeq (\mathbb{N}, +)$.

$$\begin{aligned}\phi([n + 1, 1]\odot[m + 1, 1]) &= \phi(\ [(n + 1)(m + 1) + (1)(1), (1)(m + 1) + (n + 1)(1)]\ ) \\ &= \phi([nm + n + m + 1 + 1, m + 1 + n + 1]) \\ &= \phi([nm + 1, 1]) \\ &= nm \\ &= \phi([n + 1, 1])\phi([m + 1, 1])\end{aligned}$$

Hence, $(\mathbb{N}_{\mathbb{Z}},\odot) \simeq (\mathbb{N}, .)$.

(iv) For every $[n, m]\in \mathbb{Z}$, take $[n+1, 1], [m+1, 1]\in \mathbb{N}_{\mathbb{Z}}$. Then

$$\begin{aligned}[n+1, 1] \oplus (-[m+1, 1]) &= [n+1, 1] \oplus [1, m+1] \\ &= [(n+1)+1, 1+(m+1)] \\ &= [n, m]\end{aligned}$$

Q.E.D

We also define the set of 'negative integers' below:

Defn: We define the subset $-\mathbb{N}_{\mathbb{Z}}$ of $\mathbb{Z}$ by $-\mathbb{N}_{\mathbb{Z}}:= \{ -[n, m] \mid [n, m] \in \mathbb{N}_{\mathbb{Z}} \}$

We will prove one more theorem which tells us that $\mathbb{Z}$ can actually be partitioned disjointedly into $\mathbb{N}_{\mathbb{Z}}$, $-\mathbb{N}_{\mathbb{Z}}$ and $\{[1, 1]\}$.

Theorem:

$\mathbb{N}_{\mathbb{Z}} \cup(-\mathbb{N}_{\mathbb{Z}}) \cup\{[1,1]\}=\mathbb{Z}$, where $\mathbb{N}_{\mathbb{Z}}$, $-\mathbb{N}_{\mathbb{Z}}$, $\{[1,1]\}$are pairwise disjoint.

Obviously, $\mathbb{N}_{\mathbb{Z}} \cup(-\mathbb{N}_{\mathbb{Z}}) \cup\{[1,1]\}\subseteq \mathbb{Z}$

Take any $z\in \mathbb{Z}$. Then there exist $x, y\in \mathbb{N}_{\mathbb{Z}}$ s.t $z =x\oplus(-y)$

Let ϕ be the isomorphism from $(\mathbb{N}, +)$ to $(\mathbb{N}_{\mathbb{Z}}, \oplus)$. Then $\phi(x')=x$, $\phi(y')=y$ for one and only one $x',y'\in \mathbb{N}$. We consider 3 cases.

(i) $x'= y'$

Since ϕ is one-one, we must also have $x= y$. This means $z= x\oplus(-x) =[1,1]$.

(ii) $x'> y'$

Then $\exists\ k' \in \mathbb{N}$ s.t $x'= y'+ k'$. By isomorphism, $\phi(x')= \phi(y')\oplus \phi(k')$. Note that $\phi(k')=k$ for some $k\in \mathbb{N}_{\mathbb{Z}}$. Then $z=(y\oplus k) \oplus(-y)=k$ and so $z\in \mathbb{N}_{\mathbb{Z}}$.

(iii) $y'> x'$

Then $\exists\ k' \in \mathbb{N}$ s.t $y' = x' + k'$. By isomorphism, $\phi(y') = \phi(x') \oplus \phi(k')$ where $\phi(k')=k$ for some $k \in \mathbb{N}_{\mathbb{Z}}$. Then $z = x \oplus (-(x \oplus k)) = x \oplus (-x) \oplus (-k) = -k$ and so $z \in -\mathbb{N}_{\mathbb{Z}}$.

Hence, $\mathbb{N}_{\mathbb{Z}} \cup (-\mathbb{N}_{\mathbb{Z}}) \cup \{[1,1]\} \supseteq \mathbb{Z}$ and so $\mathbb{N}_{\mathbb{Z}} \cup (-\mathbb{N}_{\mathbb{Z}}) \cup \{[1,1]\} = \mathbb{Z}$.

By definition of $\mathbb{N}_{\mathbb{Z}}$, if $[1,1] \in \mathbb{N}_{\mathbb{Z}}$, then $\exists\ k \in \mathbb{N}$ s.t $k+1=1$. But this is impossible in $\mathbb{N}$! If $[1,1] \in (-\mathbb{N}_{\mathbb{Z}})$, then $[1,1] = -[1,1] \in \mathbb{N}_{\mathbb{Z}}$ which gives the same contradiction as the preceding result. Finally, take $x \in \mathbb{N}_{\mathbb{Z}} \cap (-\mathbb{N}_{\mathbb{Z}})$. Since $x \in -\mathbb{N}_{\mathbb{Z}}$, $-x \in \mathbb{N}_{\mathbb{Z}}$ and by closure of $\mathbb{N}_{\mathbb{Z}}$ under $\oplus$, $[1,1] = x \oplus (-x) \in \mathbb{N}_{\mathbb{Z}}$ which gives the same contradiction again.

Hence, $\mathbb{N}_{\mathbb{Z}}$, $-\mathbb{N}_{\mathbb{Z}}$, $\{[1,1]\}$are pairwise disjoint.

Q.E.D

We are now ready to define a meaningful order on $\mathbb{Z}$.

Defn: Let m, n$\in\mathbb{Z}$. We say m is larger than n or n is smaller than m, and we write $m \succ n$ if $m \oplus (-n) \in \mathbb{N}_{\mathbb{Z}}$. We write $m \succcurlyeq n$ whenever $m = n$ or $m \succ n$.

The following theorem, which is in fact an easy consequence of the preceding two theorems, tells us that $(\mathbb{Z}, \oplus, \odot, \succ)$ is actually an ordered integral domain.

Theorem:

$(\mathbb{Z}, \oplus, \odot, \succ)$ is an ordered integral domain.

We need only show that $\mathbb{N}_{\mathbb{Z}}$ satisfy

c) $\forall x, y \in \mathbb{N}_{\mathbb{Z}}$, $x \oplus y$, $x \odot y \in \mathbb{N}_{\mathbb{Z}}$

d) $\forall x \in \mathbb{Z}$, one and only one of the following holds: $x \in \mathbb{N}_{\mathbb{Z}}$,$x=[1,1]$, $-x \in \mathbb{N}_{\mathbb{Z}}$

a) is true since we have shown that $\mathbb{N}_{\mathbb{Z}}$ is closed under $\oplus$ and $\odot$. b) is true since $\mathbb{Z} = \mathbb{N}_{\mathbb{Z}} \cup (-\mathbb{N}_{\mathbb{Z}}) \cup \{[1,1]\}$ and $\mathbb{N}_{\mathbb{Z}}$, $-\mathbb{N}_{\mathbb{Z}}$ and $\{[1,1]\}$ are pair-wise disjoint.

Hence, $(\mathbb{Z}, \oplus, \odot, \succ)$ is an ordered integral domain.

Q.E.D

Unlike what we did in $\mathbb{N}$, we will prove no order properties here. Since we have shown that $\mathbb{Z}$ is an ordered integral domain, we can always 'borrow' the properties that we have proven for an ordered integral domain in the general proof section. In our subsequent developments, this situation will still persist. This is due to the fact that the integers, rationals and the reals all fit into nice general mathematical structures. The construction of $\mathbb{N}$ was a bit more cumbersome and less elegant since nobody has yet bothered to come up with a general structure resembling it!

The Integer System

We have shown one particular way to construct a system that models the integers. Given just the set of natural numbers, two different persons might come up with two methods to construct a system that they think models the integers. But what actually is the essence of the integers? We hope that the reader will agree with us that whatever system that one can come up with, it must at least be an ordered integral domain. Furthermore, it should contain a 'copy' of the natural numbers that serves as its positive elements. Besides that, one should be able to write every element in the set as the difference of two natural numbers. We make this intuition more precise in the definition below:

Defn: An ordered integral domain $(X, \oplus, \odot, \succ)$ is called an integer system if $\exists$ a subset $\mathbb{N}_X$ of X such that

(i) Both $(\mathbb{N}_X, \oplus)$ and $(\mathbb{N}_X, \odot)$ are semi-groups and under the same isomorphism $\phi: \mathbb{N}_X \to \mathbb{N}$, we have $(\mathbb{N}_X, \oplus) \simeq (\mathbb{N}, +)$ and $(\mathbb{N}_X, \odot) \simeq (\mathbb{N}, .)$ as semi-group. Furthermore, for every x, y $\in \mathbb{N}_X$, we have $x \succ y \Rightarrow \phi(x) > \phi(y)$

(ii) For every $x \in X$, $\exists$ y, $z \in \mathbb{N}_X$ s.t $x = y \oplus (-z)$

We will now show that our Net Difference System is actually an integer system. Furthermore, we will show that any two integer systems are isomorphic and so there is essentially only one integer system. The uniqueness of integer systems reinforces our belief that our intuition about what constitute the fundamental properties of the integers is correct. At the very least, it will be more desirable than other criteria that allows one to generate two systems with different properties! We first give a formal proof of our claims.

Theorem: Existence And Uniqueness Of Integer Systems.

Integer systems exist and any two integer systems are isomorphic.

We claim that $(\mathbb{Z}, \oplus, \odot, \succ)$ is an integer system. Consider the subset $\mathbb{N}_\mathbb{Z}$. We have already shown that both $(\mathbb{N}_\mathbb{Z}, \oplus)$ and $(\mathbb{N}_\mathbb{Z}, \odot)$ are semi-groups and that they are isomorphic to $(\mathbb{N}, +)$ and $(\mathbb{N}, .)$ respectively under the same isomorphism $\phi: \mathbb{N}_\mathbb{Z} \to \mathbb{N}$ defined by

$\phi([n+1, 1]) = n$

For every $[n+1,1], [m+1,1] \in \mathbb{N}_\mathbb{Z}$, we have

$$\begin{aligned}[n+1,1] \succ [m+1,1] &\Rightarrow [n+1,1] \oplus (-[m+1,1]) \in \mathbb{N}_\mathbb{Z}\\ &\Rightarrow [n+1,1] \oplus [1, m+1] \in \mathbb{N}_\mathbb{Z}\\ &\Rightarrow [(n+1)+1, 1+(m+1)] \in \mathbb{N}_\mathbb{Z}\\ &\Rightarrow [n, m] \in \mathbb{N}_\mathbb{Z}\end{aligned}$$

This means $[n, m] = [k+1, 1]$ for some $k \in \mathbb{N}$. Hence, $(n, m) \sim (k+1,1)$ and so $n+1 = m+(k+1)$, i.e $n = m+k$ and so $n>m$. Hence, $[n+1,1] \succ [m+1,1] \Rightarrow \phi([n+1, 1]) > \phi([m+1, 1])$. Also, we have shown that for every $x \in \mathbb{Z}$, $\exists$ y, $z \in \mathbb{N}_\mathbb{Z}$ s.t $x = y \oplus (-z)$.

Hence, we conclude that $(\mathbb{Z}, \oplus, \odot, \succ)$ is an integer system and so integer systems exist.

Let $(\mathbb{Z}, \oplus, \odot, \succ)$ and $(\mathbb{Z}', \oplus', \odot', \succ')$ be any 2 integer systems. By transitivity of isomorphism through $(\mathbb{N}, +, ., >)$ (note that we employed a uniform isomorphism in the definition of integer systems), $\exists$ an isomorphism $\phi: \mathbb{N}_\mathbb{Z} \to \mathbb{N}_{\mathbb{Z}'}$ s.t $\forall$ y, $z \in \mathbb{N}_\mathbb{Z}$,

$\phi(y \oplus z) = \phi(y) \oplus' \phi(z)$

$\phi(y \odot z) = \phi(y) \odot' \phi(z)$

$y \succ z \Rightarrow \phi(y) \succ' \phi(z)$

Also, for any $x \in \mathbb{Z}$, $\exists\ y_x, z_x \in \mathbb{N}_{\mathbb{Z}}$ s.t $x = y_x \oplus (-z_x)$.

Define $\psi: \mathbb{Z} \to \mathbb{Z}'$ by
$\psi(x) = \phi(y_x) \oplus' (-\phi(z_x))$

For any $a, b \in \mathbb{Z}$,
Suppose that $a = b$. Then
$y_a \oplus (-z_a) = y_b \oplus (-z_b)$
$\Rightarrow y_a \oplus z_b = y_b \oplus z_a$
$\Rightarrow \phi\ (y_a \oplus z_b) = \phi(y_b \oplus z_a)$
$\Rightarrow \phi(y_a) \oplus' \phi(z_b) = \phi(y_b) \oplus' \phi(z_a)$
$\Rightarrow \phi(y_a) \oplus' (-\phi(z_a)) = = \phi(y_b) \oplus' (-\phi(z_b))$
$\Rightarrow \psi(a) = \psi(b)$
Hence ψ is well-defined.
Suppose that $\psi(a) = \psi(b)$. Then
$\phi(y_a) \oplus' (-\phi(z_a)) = \phi(y_b) \oplus' (-\phi(z_b))$
$\Rightarrow \phi(y_a) \oplus' \phi(z_b) = \phi(y_b) \oplus' \phi(z_a)$
$\Rightarrow \phi\ (y_a \oplus z_b) = \phi(y_b \oplus z_a)$
$\Rightarrow y_a \oplus z_b = y_b \oplus z_a$ (Since ϕ is one-one)
$\Rightarrow y_a \oplus (-z_a) = y_b \oplus (-z_b)$
$\Rightarrow a = b$
Hence, ψ is one-one.

Take any $x' \in \mathbb{Z}'$. Then $x' = y_{x'} \oplus' (-z_{x'})$. Since ϕ is onto $\mathbb{N}_{\mathbb{Z}'}$, $\exists\ y, z \in \mathbb{N}_{\mathbb{Z}}$ s.t $\phi(y) = y_{x'}$, $\phi(z) = z_{x'}$.

Take $x = y \oplus (-z) \in \mathbb{Z}$. Then
$\psi(x) = \psi(y \oplus (-z))$
$= \phi(y) \oplus' (-\phi(z))$
$= y_{x'} \oplus' (-z_{x'})$
$= x'$
Hence, ψ is onto.
Hence ψ is a bijective function.

For any $a, b \in \mathbb{Z}$,
$\psi(a \oplus b) = \psi(\ (y_a \oplus (-z_a)) \oplus (y_b \oplus(-z_b))\ )$
$= \psi(\ (y_a \oplus y_b) \oplus (-(z_a \oplus z_b))\ )$
$= \phi(y_a \oplus y_b) \oplus' (-\phi(z_a \oplus z_b))$
$= (\phi(y_a) \oplus' \phi(y_b)) \oplus' (-(\phi(z_a) \oplus' \phi(z_b))\ )$
$= \phi(y_a) \oplus' \phi(y_b) \oplus' (-\phi(z_a)) \oplus' (-\phi(z_b))$
$= (\ \phi(y_a) \oplus' (-\phi(z_a))\ ) \oplus' (\ \phi(y_b) \oplus' (-\phi(z_b))\ )$
$= \psi(a) \oplus' \psi(b)$

$\psi(a \odot b) = \psi(\ (y_a \oplus (-z_a)) \odot (y_b \oplus (-z_b))\ )$
$= \psi((y_a \odot y_b) \oplus (y_a \odot (-z_b)) \oplus ((-z_a) \odot y_b) \oplus ((-z_a) \odot (-z_b))\ )$
$= \psi(\ ((y_a \odot y_b) \oplus (z_a \odot z_b)) \oplus (-((y_a \odot z_b) \oplus (z_a \odot y_b)))\ )$
$= \phi((y_a \odot y_b) \oplus (z_a \odot z_b)) \oplus' (-\phi((y_a \odot z_b) \oplus (z_a \odot y_b))\ )$
$= (\phi(y_a \odot y_b) \oplus' \phi(z_a \odot z_b)) \oplus' (-(\phi(y_a \odot z_b) \oplus' \phi(z_a \odot y_b))\ )$
$= \phi(y_a \odot y_b) \oplus' \phi(z_a \odot z_b) \oplus' (-\phi(y_a \odot z_b)) \oplus' (-\phi(z_a \odot y_b))$

$$= (\phi(y_a)\odot' \phi(y_b)) \oplus' (\phi(z_a)\odot'\phi(z_b)) \oplus' (\phi(y_a)\odot'(-\phi(z_b))) \oplus'((-\phi(z_a))\odot' \phi(y_b))$$
$$= (\phi(y_a)\odot'\phi(y_b))\oplus'(\phi(y_a)\odot'(-\phi(z_b)))\oplus'((-\phi(z_a))\odot'\phi(y_b))\oplus'((-\phi(z_a))\odot'(-\phi(z_b)))$$
$$= (\phi(y_a) \oplus' (-\phi(z_a))) \odot' (\phi(y_b) \oplus' (-\phi(z_b)))$$
$$= \psi(a) \odot' \psi(b)$$

$$a \succ b \Rightarrow y_a \oplus (-z_a) \succ y_b \oplus (-z_b)$$
$$\Rightarrow y_a \oplus z_b \succ y_b \oplus z_a$$
$$\Rightarrow \phi(y_a \oplus z_b) \succ' \phi(y_b \oplus z_a)$$
$$\Rightarrow \phi(y_a) \oplus' \phi(z_b) \succ' \phi(y_b) \oplus' \phi(z_a)$$
$$\Rightarrow \phi(y_a) \oplus' (-\phi(z_a)) \succ' \phi(y_b) \oplus' (-\phi(z_b))$$
$$\Rightarrow \psi(a) \succ' \psi(b)$$

Hence, ψ is an isomorphism from $(\mathbb{Z}, \oplus, \odot, \succ)$ to $(\mathbb{Z}', \oplus', \odot', \succ')$.

Hence $(\mathbb{Z}, \oplus, \odot, \succ) \simeq (\mathbb{Z}', \oplus', \odot', \succ')$.

Q.E.D

From now on, we will abandon our Net Difference System and consider instead the general integer system. We will denote the integer system by $(\mathbb{Z}, +, ., >)$. The 'copy' of the natural numbers embedded in $\mathbb{Z}$ will still be denoted by $\mathbb{N}$ and it has all the properties that we have proven in chapter 1 if we consider it in isolation. The concern that we do not differentiate the binary and order notation for the integer system and the 'original' natural system is unfounded, since we now have no need to refer to the 'original' natural system from which the specific Net Difference System was built at all. That does not mean we have abandoned the natural system. We still need it a lot, but there is now a sub-structure $(\mathbb{N}, +, ., >)$ in $(\mathbb{Z}, +, ., >)$ which we can use as our new model for the natural system. As we have proven in Chapter 1, any two natural number systems are isomorphic and so this changing of models has no effect other than making the construction process more elegant. We will now proceed to define concepts unique to the integer system and prove their associated results.

Traditional Concepts Associated With Integers.

Most of us are familiar with the concept of a prime number, divisors and greatest common divisors. We also know that these are concepts associated with 'whole numbers', which essentially means the integers. Also, the fundamental theorem of arithmetic is actually a result regarding the integers. Hence, our integer system should be able to accommodate all these concepts also. In this section, we will show that such concepts really are valid and do make sense in our integer system. Let us start by showing that $\mathbb{Z}$ is 'discrete'.

Theorem:

For $n\in\mathbb{Z}$, $\nexists\, m\in\mathbb{Z}$ s.t $n < m < n + 1$.

First, we show that for $n\in \mathbb{N}$, $\nexists\, m\in \mathbb{Z}$ s.t $n < m < n + 1$.

By transitivity, $m\in \mathbb{N}$ if it exists. But we have already shown this to be impossible for $\mathbb{N}$, and so the result holds here also.

Now, assume such an m exists. Then

$n < m < n + 1$

$\Rightarrow n+(-n+1) < m +(-n+1) < n+1 +(-n+1)$

$\Rightarrow 1 < m - n + 1 < 1+ 1$

This of course is not possible since $1 \in \mathbb{N}$. Hence, such an m cannot exist.

Q.E.D

The pigeonhole principle tells us that intervals in $\mathbb{N}$ is finite. We will show here that it is true also for intervals in $-\mathbb{N}$, the set of negative integers.

Lemma:

The intervals [-n, -1] is finite for every $n \in \mathbb{N}$.

We define $f:[1,n] \rightarrow [-n,-1]$ by

$f(x)= -x \qquad \forall\ x \in [1, n]$

Since $1 \le x \le n \Leftrightarrow -n \le -x \le -1$ and due to the fact that the negative is unique, f must be a well-defined bijective function. By the pigeonhole principle, [1,n] is finite and so [-n,-1] will be finite also.

Q.E.D

As in the case for $\mathbb{N}$, the following theorem tells us that $\mathbb{Z}$ is completely ordered.

Theorem:

For any non-empty subset E of $\mathbb{Z}$, the following holds:

(i) If E is bounded above, SupE exists and SupE∈E.

(ii) If E is bounded below, InfE exists and InfE∈E.

(iii) E is finite iff E is both bounded above and below.

(i) Let E be bounded above by k. Since E is non-empty, $\exists\ x_0 \in E$. Consider the set $A = \{n \in \mathbb{N} \mid x_0 + n-1 \in E\}$. Then A is a non-empty subset of $\mathbb{N}$ since $1 \in A$. Also, A is bounded above by $k + 1 - x_0\ (\in \mathbb{N})$. Hence by order completeness of $\mathbb{N}$, SupA exists and SupA∈A. This means x_0 + SupA-1∈E and obviously, x_0 + SupA-1 is an upper bound for E. Hence MaxE = x_0 +SupA-1 and so the assertion is true.

(ii) Let E be bounded below by k. Consider the set $L=\{x \in \mathbb{Z} \mid x$ is a lower bound of $E\}$. L is non-empty since $k \in L$. Also, as E is also non-empty, $\exists\ y_0 \in E$ that bound L from above. Hence, by (i), SupL exists and is in L. Now, consider SupL + 1. Since SupL + 1 > SupL, SupL + 1∉L and so $\exists\ y_1 \in E$ s.t $y_1 <$ SupL + 1. This means SupL $\le y_1 <$ SupL + 1. Since we cannot have SupL $< y_1 <$ SupL + 1, it follows that SupL = y_1. Hence MinE = SupL and so the assertion is true.

(iii) Let E be finite. Then the sets $E \cap \mathbb{N}$, $E \cap (-\mathbb{N})$ are also finite. If $E \cap \mathbb{N} = \phi$, then 0 is an upper bound for E. Otherwise, $E \cap \mathbb{N}$ is bounded above by some $k \in \mathbb{N}$. This means k is also an upper bound for E. Similarly, if $E \cap (-\mathbb{N}) = \phi$, then 0 is a lower bound for E. Otherwise, $E \cap (-\mathbb{N})$ is bounded below by some $l \in -\mathbb{N}$ and so E is bounded below by l.

Suppose now that E is bounded above and below by k and l respectively. We consider 3 cases.

(a) $k, l \in \mathbb{N} \cup \{0\}$.

Then E is a subset of the finite set $[1, k] \cup \{0\}$ and so is finite

(b) k, $l \in -\mathbb{N} \cup \{0\}$.

Then E is a subset of the finite set $[l, -1] \cup \{0\}$ and so is finite.

(c) $k \in \mathbb{N} \cup \{0\}$, $l \in -\mathbb{N} \cup \{0\}$.

Then E is a subset of the finite set $[l, -1] \cup \{0\} \cup [1, k]$ and so is finite.

Q.E.D

Statement (i) and (ii) of the theorem tells us that $\mathbb{Z}$ is completely ordered. We will demonstrate that $\mathbb{Z}$ is not well-ordered by giving a concrete example later when we have defined the concept of divisibility. In order to demonstrate the Division Algorithm, we first require that $\mathbb{Z}$ has the Archimedean property:

Theorem: Archimedeon Property

Let m, n∈$\mathbb{Z}$, m > 0. Then ∃ k∈$\mathbb{N}$ s.t mk > n.

We consider 2 cases.

(i) $n > 0$

This follows directly from the Archimedeon Property for $\mathbb{N}$.

(ii) $n \le 0$

Take $k = 1$ and $mk = m > 0 \ge n$.

Hence the Archimedeon Property for $\mathbb{Z}$ holds.

Q.E.D

Theorem: Division Algorithm

Let m, n∈$\mathbb{Z}$, n > 0. Then ∃ unique integers q and r s.t 0 ≤ r < n and m = nq + r.

Let $A := \{m + nq \mid q \in \mathbb{Z}, m + nq \ge 0\}$. Then A is a non-empty subset of $\mathbb{N} \cup \{0\}$ since by the Archimedeon Property for $\mathbb{Z}$, $\exists$ $k \in \mathbb{Z}$ s.t $nk > -m$, i.e $m + nk > 0$. Hence, since $\mathbb{N}$ is well-ordered, $\mathbb{N} \cup \{0\}$ is also well-ordered and so A has a minimum, r. We then have $m + nq = r$ for some $q \in \mathbb{Z}$. Clearly, $r \ge 0$ by definition. Suppose $r > n$. Then, since both n, $r \in \mathbb{N}$, $\exists$ $r_1 \in \mathbb{N}$ s.t $r = n + r_1$. This also mean that $r > r_1$. Now

$r_1 = r - n = m + nq - n = m + (q - 1)n$.

This mean $r_1 \in A$ which contradict r being the minimum for A. Hence $\exists$ q, $r \in \mathbb{Z}$ s.t

$m = nq + r$ with $0 \le r < n$.

Suppose that $nq + r = nq_1 + r_1$ where $0 \le r, r_1 < n$.

Let $r < r_1$.

Then $0 < r_1 - r < n\text{-}r < n$ and $r_1 - r = n(q - q_1)$. Then $q - q_1 > 0$. We also have $n(q - q_1) < n(1)$, i.e $0 < q - q_1 < 1$ which is impossible. By symmetry, $r > r_1$ is also impossible. Hence, $r = r_1$. As a result, $q = q_1$ also and so the representation is unique.

Q.E.D

We will now define formally the concept of a divisor and prove some simple results associated with it.

Defn: An integer n ≠ 0 is called a divisor (or a factor) of an integer m (or we say n divides m) if ∃ an integer q such that m = nq. We write n | m if n divides m.

Theorem:

For m, n∈ℤ, the following holds:

(i) If n | m, then there is exactly one integer q s.t m = nq

(ii) If m ≠ 0, m is divisible by m, -m, 1 and –1.

(iii) If n | m and m | k, then n | k.

(iv) If n | m and n | k, then n | (m+k) and n | (m-k)

(v) If n | (m+k) and n | m, then n | k

(vi) If n| m, then kn| km, k ≠ 0

(vii) If n| m, then n| mk

(i) Since n ≠ 0, we have $nq_1 = nq_2 \Rightarrow q_1 = q_2$ and so the assertion is true.

(ii) The statement is true by the following equality:
m = (m)(1) = (-m)(-1).

(iii) ∃ q_1, q_2 s.t $m = nq_1$ and $k = mq_2$. Then $k = n(q_1q_2)$ and so n | k.

(iv) ∃ q_1, q_2 s.t $m = nq_1$ and $k = nq_2$. Since $m + k = n(q_1 + q_2)$ and $m–k = n(q_1– q_2)$, we have n | (m + k), n | (m – k) also.

(v) We can write k = (m + k) – m and so the result follows from (iv).

(vi) ∃ q s.t m = nq. Then km = (kn)q and so kn | km.

(vii) ∃ q s.t m = nq. Then km = (kq)n and so n | mk.

Q.E.D

We can now show that ℤ is not well-ordered by basically considering the set of even integers.

Theorem: ℤ is not well-ordered.

The set A={n∈ℤ | 2|n} is nonempty but MinA does not exist.

Now, 2∈A so A is not empty. Suppose that MinA exist. Since 2|2 and 2|MinA, we have 2|(MinA-2). This means MinA-2∈A which is a contradiction since
MinA-2< MinA. Hence MinA cannot exist.

Q.E.D

With the concept of a divisor, we can now say precisely what is meant by a prime number.

Defn: An integer p > 1 is called a prime if for every q∈ℕ, q | p ⇒ q = 1 or q = p. An integer p > 1 which is not a prime is called a composite number.

We will proceed to prove a lemma that will aid us in showing that every positive integer greater than 1 can be expressed as a product of primes.

Lemma:

Let n > 1. Then n is composite iff ∃ m, k∈ℕ s.t 1 < m, k < n and n = mk.

Suppose n is composite. Then ∃ m∈ℕ s.t m | n but m≠1, n. Then we can write n= mk for some k∈ℤ. Since m, n > 0, we have k > 0. Also, k =1⇒ n = m and k = n ⇒ m = 1, both of which is forbidden. Since m, k > 1, we have m, k < n. Hence, ∃ m, k∈ℕ s.t
1 < m, k < n and n = mk.

Conversely, if such m, k exists, then in particular, $m\in\mathbb{N}$ and $m \mid n$ but $m \neq 1$, n. Hence, n must be composite.

Q.E.D

Theorem: Prime factorization

Every integer $n > 1$ can be expressed as a product of primes.

Let $P = \{n\in\mathbb{N} \mid n \text{ is a product of primes or } n = 1\}$. By definition, $1\in P$. Suppose $\{k\in\mathbb{N} \mid k \leq n\} \subseteq P$. If $n + 1$ is a prime, then obviously $n + 1\in P$. Otherwise, $\exists$ p, $q\in\mathbb{N}$ s.t $n + 1 = pq$ and $1 < p, q < n + 1$. Hence, p, $q\in P$ by induction hypothesis and so both p and q are products of primes. Since $n + 1$ is the product of p and q, it must also be products of primes. Hence, $\{k\in\mathbb{N} \mid k \leq n\} \subseteq P \Rightarrow n + 1\in P$ and so by the general principle of induction, $P = \mathbb{N}$. Now, take any $n > 1$. Since $n\in P$, n is a product of primes by the defining property of P.

Q.E.D

The following definition gives us the concept of a greatest common divisor of two integers.

Defn: Let m, $n\in\mathbb{Z}$. An integer $d\in\mathbb{Z}$ is called a common divisor of n and m if $d|n$ and $d|m$. We define the greatest common divisor of m and n by

g.c.d(m, n) = $\text{Sup}D_{m,n}$, where $D_{m,n} = \{k\in\mathbb{N} \mid k \text{ is a common divisor of n and m}\}$

Theorem:

Let n, $m\in\mathbb{Z}$. Then the following hold:

(i) g.c.d(n, m), if it exists, is positive and unique.

(ii) If $d > 0$ is a common divisor of n and m, then d = g.c.d(n, m) if d is divisible by every common divisor of n and m.

(iii) g.c.d(n, m) exists iff at least one of m, n is not zero.

(iv) If g.c.d(m, n) exists, then g.c.d(m, n) = nx + my for some x, $y\in\mathbb{Z}$.

(v) If g.c.d(m, n) exists, then it is divisible by every common divisor of n and m.

(i) Being the suprema of a non-empty subset of $\mathbb{N}$ (note that $1|n$, $1|m$), it must be positive and unique whenever it exists.

(ii) For any $d_1\in D_{m,n}$, we then have $d=d_1q$ for some $q\in\mathbb{Z}$. Since d, $d_1>0$, we have $q> 0$ and so $d \geq d_1$. Also, $d\in D_{m,n}$ and so d = g.c.d(m, n).

(iii) Suppose g.c.d(m, n) exists. If both m, n are zero, then since every non-zero integer divide zero, we have $D_{m,n} = \mathbb{N}$ which is unbounded! This means g.c.d(m, n) cannot exist which is a contradiction. Conversely, suppose that at least one of them, say m, is not zero. Then $D_{m,n}$ is bounded by m and so its suprema, i.e g.c.d(m, n) will exist by order completeness of $\mathbb{N}$.

(iv) Since g.c.d(m, n) exists, then by (iii), we may assume that $n \neq 0$. Consider the set $A= \{nx + my \mid x, y\in\mathbb{Z}\}$. Let ($y = 0$) and ($x = 1$ if $n> 0$, $x = -1$ if $n< 0$). Then $nx+my>0$, i.e A has at least one positive integer. Hence, $A\cap\mathbb{N}$ is non-empty and so has a least element, a, since $\mathbb{N}$ is well-ordered. Then $a = nx_0 + my_0$ for some x_0, $y_0\in\mathbb{Z}$. Let d be a common divisor of n and m. Obviously, $d|a$. We need only show that $a\in D_{m,n}$. By division algorithm, $n = aq + r$ for some $q, r\in \mathbb{Z}$, $0 \le r < a$. Then

$n = q(nx_0 + my_0) + r$

$\Rightarrow r = n(1 - qx_0) + m(- qy_0)$, i.e $r \in A$

If $r \ne 0$, then $r\in A\cap\mathbb{N}$ and $r < a$, which contradicts the leastness of a. Hence $r = 0$, i.e. $a|n$. By symmetry, $a |m$ and so $a\in D_{m,n}$. By (ii), a = g.c.d(n, m). Note that we have shown that g.c.d (n,m) is actually the least element of the set $\{nx + my \mid x, y\in \mathbb{Z}\}$.

(v) By (iv), g.c.d(m, n) = nx + my for some $x, y\in \mathbb{Z}$. Obviously, $d\in D_{m,n} \Rightarrow$ d | g.c.d(m, n) and so the statement is true.

Q.E.D

If two integers have no 'common factor', then we would naturally expect their greatest common divisor to be 1. Such pairs of integers have a special name as defined below:

Defn: Let $n, m\in \mathbb{Z}$. We say n and m are coprime if g.c.d(n, m) = 1

<u>Theorem:</u>

Let m, n, $k\in\mathbb{Z}$. Then the following holds:

(i) g.c.d(n, m) = g.c.d(n, n+m)

(ii) g.c.d(kn, km) = kg.c.d(n, m), if k > 0

(iii) g.c.d(n, km) = 1 if g.c.d(n, k) = 1 and g.c.d(n, m) = 1.

(iv) Let g.c.d(n, m) = 1. If n | mk, then n | k.

(v) Let p be a prime. Then p | nm ⇒ p | n or p | m.

(i) Since g.c.d(n, m)| n and g.c.d(n, m)| m, g.c.d(n, m)| n+m and so g.c.d(n, m)$\in D_{n,\ n+m}$. Hence g.c.d(n, m) ≤ g.c.d(n, n+m). Similarly, since g.c.d(n, n+m) | n and g.c.d(n, n+m) | n+m, g.c.d(n, n+m) | m and so g.c.d(n, n+m)$\in D_{n,m}$, i.e g.c.d(n, n+m) ≤ g.c.d(n, m). Hence g.c.d(n, m) = g.c.d(n, n+m).

(ii) Since g.c.d(n, m) | n and g.c.d(n, m) | m, kg.c.d(n, m) | kn and kg.c.d(n, m) | km so that kg.c.d(n, m)$\in D_{kn,\ km}$ (since kg.c.d(n, m) > 0). Now, let $d\in D_{kn,\ km}$. Note that g.c.d(n, m) = nx + my for some $x, y\in \mathbb{Z}$, i.e. kg.c.d(n, m) = knx + kmy. Since d | kn (and hence d | knx) and d | km(and hence d | kmy), d | (knx + kmy). Hence, kg.c.d(n, m) = g.c.d(kn, km).

(iii) We can write $nx_1 + ky_1 = 1 = nx_2 + my_2$ for some $x_1, y_1, x_2, y_2\in \mathbb{Z}$. Then we have

$(nx_1 + ky_1)(nx_2 + my_2) = (1)(1)$

$\Rightarrow (nx_1)(nx_2) + (nx_1)(my_2) + (ky_1)(nx_2) + (ky_1)(my_2) = 1$

$\Rightarrow n(nx_1x_2 + mx_1y_2 + ky_1x_2) + (mk)(y_1y_2) = 1$

Since g.c.d(n, km)| n and g.c.d(n, km)| mk, it must divide the above expression, i.e.1. Hence 0 < g.c.d(n, km) ≤ 1 and so g.c.d(n, km) = 1.

(iv) $\exists$ $x, y\in \mathbb{Z}$ s.t nx + my = 1. Then nkx + mky = k. Since n | n (and hence nkx) and n | mk (and hence mky), n must divide their sum, i.e. k.

(v) Now, g.c.d(p, n) is either 1 or p by definition. If g.c.d(p, n) = p, then p | n. Otherwise, g.c.d(p, n) = 1 and by (iv), p | m.

Q.E.D

We will end this section with the fundamental theorem of arithmetic. Although the name sounds impressive, it is really quite an intuitive result and we have already proved part of it in our prime factorization theorem. We requires the following lemma to make our job simpler:

Lemma:

Let p be a prime s.t $p \mid x_1x_2... x_n$, where each $x_i \in \mathbb{Z}$. Then p divides at least one x_i , $1 \leq i \leq n$.

Let $P = \{n \in \mathbb{N} \mid p \mid x_1x_2... x_n \Rightarrow p \mid x_i$ for some $1 \leq i \leq n\}$. Clearly, $1 \in P$.

Suppose that $\{ n \in \mathbb{N} \mid n \leq k\} \subseteq P$. For any $x_1, x_2, ..., x_{k+1} \in \mathbb{Z}$, let $p \mid x_1x_2... x_{k+1}$. Then either $p \mid x_1x_2... x_n$ (in which case $p \mid x_i$ for some $1 \leq i \leq k$ by induction hypothesis) or $p \mid x_{k+1}$. Hence $k + 1 \in P$ whenever $\{n \in \mathbb{N} \mid n \leq k\} \subseteq P$ and so by the general principle of induction, $P = \mathbb{N}$ and so the assertion is true.

Q.E.D

The above lemma actually allows us to obtain the following result which will be employed in Chapter 3 easily:

Lemma:

$2|n$ iff $2| n^2$

$2| n^2 \Leftrightarrow 2|n$ or $2| n$

$\Leftrightarrow 2|n$

Q.E.D

Finally, let us now prove the fundamental theorem of arithmetic.

Fundamental Theorem of Arithmetic

Let n > 1 be any integer. Then n can always be expressed as a product of primes and this prime factorization is unique except for a possible change of order.

We have already shown that any integer n > 1 can be expressed as a product of primes.

Let $P = \{n \in \mathbb{N} \mid$ the prime factorization for n is unique$\}$. Clearly, $2 \in P$ since there is obviously only one prime factorization, i.e. 2 = 2. Suppose that $\{n \in \mathbb{N} \mid n \leq k\} \subseteq P$. If k + 1 is a prime, then $k + 1 \in P$. Otherwise, let L_{k+1} and R_{k+1} be two prime factorization for k + 1. Take any particular prime p that occurs in L_{k+1}. Then $p \mid R_{k+1}$ and so p must divide some prime q that occur in R_{k+1}. Since q is a prime and p>1, it follows that p=q. Remove p from L_{k+1} (and form L_{k+1}') and q from R_{k+1} (and form R_{k+1}'). Then L_{k+1}' and R_{k+1}' are both prime factorization for some integer $1 < m < k + 1$ and by induction hypothesis, both are the same prime factorization. Hence L_{k+1} and R_{k+1} are also the same prime factorization for k+1 since they are both created from L_{k+1}' and R_{k+1}' by introducing the prime p.

Hence, $k + 1 \in P$ whenever $\{n \in \mathbb{N} \mid n \leq k\} \subseteq P$. By the modified and general principle of induction, $P = \mathbb{N} \backslash \{1\}$ and so the theorem is proved.

Q.E.D

Inadequacy Of ℤ

As we have done for the natural system, we must find some fault with the integer system so that there is a motivation to carry on with our construction. This is not really a difficult task, since it is obvious that we cannot do division in ℤ just as we cannot do subtraction in ℕ. Intuitively, subtraction is the reverse process of addition and when we subtract 3 from 5, we are really asking for the number that when added to 3 gives 5. Similarly, we can phrase division in terms of multiplication that has already been defined in ℤ. This will help us see technically that ℤ really has not enough elements for a self contained division mechanism. For illustration, let us ask for the result of 5 divided by 3. This reduces to finding an integer that when multiplied by 3 gives 5. Due to properties of order, this integer, n, must be a positive quantity. It cannot be 1 since that will make 3 the equal of 5, which is obviously not true. Hence, we can write n as the product of primes P_n. As 3 is a prime, this makes $3P_n$ a prime factorization for 5. As 5 is already a prime, its prime factorization must be itself. We can still avoid disaster if a positive integer greater than 1 can have a lot of different prime factorizations but as luck would have it, the fundamental theorem of Arithmetic explicitly expressed its disapproval. So on the one hand, we have a prime factorization that consist only of the prime 5 and another with at least 2 primes, one of which is 3. There is no way that one can pretend that the prime 3 lives in a house that everybody knows belong only to the prime 5 and so we have our contradiction. Hence, division does not appear to be a job suitable for the residents in ℤ. Whenever they undergoes division, they almost always fell off the edge of the world!

The next chapter will pursue the goal of extending the integer system so that one can do division in the new system. Of course, the new system will still not allow us to ‘divide by zero’, but that is a restriction that one’s intuition can easily give a justification. Division by lessor things gives bigger share. If we divide by nothing, then what we get must be something infinitely large, and an infinite fat element is a bully not welcomed by the rest of the elements in our new system.

End of Chapter 2

CHAPTER 3: FIELDS OF RATIONALS

Introduction

The rational numbers are really nothing more than the fractions that we are taught in elementary school. At a very young age, we know that life is not always fair and sometimes, you just have to get one sweet lesser than your brother since 7 cannot be divided evenly into 2 parts and your brother happen to be the bigger of the two. This may be tolerable when one is talking about sweets but in the real world, 'one whole' can indeed be a very huge quantity and an uneven distribution can turn out to be very unfair indeed! Hence, the concept of a 'fractional part' was conceived and this leads to a whole system of rational numbers which we are going to construct in this chapter.

The Fractional System

We already have an integer system with its set of integers $\mathbb{Z}$. As we did while creating the Net Difference System, we are going to split ordered pairs of integers into equivalence classes. Each equivalence class resides pairs that give the same result when the first integer is 'divided' by the latter. For any pairs, we forbid the zero integer to be used for the second integer since that would represent 'division by zero'. The precise definition of our new set is given below:

Defn: We say two elements (m, n), (p, q)$\in \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ are related to each other and write (m, n) ~ (p, q) if mq = np.

As we have claimed, this partition is an equivalence relation:

Theorem:

The relation ~ is an equivalence relation on $\mathbb{Z}\times(\mathbb{Z}\backslash\{0\})$

Since mn = nm $\forall$ n, m$\in\mathbb{Z}$, ~ is reflexive.

Let (m, n) ~ (p, q). Then

mq = np $\Rightarrow$ pn = qm

$\Rightarrow$ (p, q) ~ (m, n)

Hence, ~ is symmetric.

Let (m, n) ~ (p, q) and (p, q) ~ (k, l). Then mq = np and pl = qk. We have mq$l$ = np$l$ and pln = qkn so that mq$l$ = qkn. Hence, ml = nk since q≠0 and so (m, n) ~ (k, l).

Hence, ~ is transitive.

Hence, ~ is an equivalence relation on $\mathbb{Z}\times(\mathbb{Z}\backslash\{0\})$.

Q.E.D

We will denote the set $(\mathbb{Z}\times(\mathbb{Z}\backslash\{0\}))/\sim$ in our Fractional System by $\mathbb{Q}$. An element [(n,m)] in $\mathbb{Q}$ will now be simply written as [n, m]. To make it a system, we need to define binary operations and an order on it as we have done for the Net Difference System. Before we do that, it will help to note some simple relations between elements in $\mathbb{Q}$.

Theorem: Elementary Properties of $\mathbb{Q}$

For [n, m], [p, q]$\in\mathbb{Q}$, the following holds:

(1) [p, q] = [kp, kq] $\forall$ k$\in\mathbb{Z}$, k $\neq$ 0.

Since k $\neq$ 0 and q $\neq$ 0, kq $\neq$ 0 and so [kp, kq]$\in\mathbb{Q}$. Obviously, p(kq) = q(kp) and so [p, q] = [kp, kq]

(2) If [n, m] = [p, q] and n, m are coprime, then p = nk and q = mk for some k$\in\mathbb{Z}$, k $\neq$ 0.

We have nq = mp. If n = 0, then 0 = nq = mp. Since m $\neq$ 0, p = 0. Similarly, p = 0 $\Rightarrow$ n = 0. Hence n = 0 $\Leftrightarrow$ p = 0. Now, observe that m|nq. Since m, n is coprime, it follows that m|q, i.e. q = mk for some k$\in\mathbb{Z}$, k $\neq$ 0 (since q $\neq$ 0). We consider 2 cases.

(i) p = 0, n = 0

Then 0 = p = nk and q = mk

(ii) p $\neq$ 0, n $\neq$ 0.

Then nmk = mp. This mean nk = p since n, m, k, p $\neq$ 0.

(3) [n, m] = [0, 1] iff n = 0

[n, m] = [0, 1] $\Leftrightarrow$ n1 = m0 $\Leftrightarrow$ n = 0.

(4) [n, m] = [1, 1] iff n = m

[n, m] = [1, 1] $\Leftrightarrow$ n1 = m1 $\Leftrightarrow$ n = m.

Q.E.D

Binary Operation on $\mathbb{Q}$

We will define here addition and multiplication on the set $\mathbb{Q}$. As in the case for $\mathbb{Z}$, a little arithmetic will enable us to guess the 'correct' definition easily.

Theorem: Addition on $\mathbb{Q}$

$\exists$ a well-defined binary operation $\oplus$ on $\mathbb{Q}$ given by

[n, m] $\oplus$ [p, q] = [nq + mp, mq] $\forall$ n, m, p, q$\in\mathbb{Z}$, m, q $\neq$ 0.

Let $[n_1, m_1] = [n_2, m_2]$ and $[p_1, q_1] = [p_2, q_2]$ where $m_1, m_2, q_1, q_2 \neq 0$.
Then $n_1m_2 = m_1n_2$ and $p_1q_2 = p_2q_1$. Thus

$[n_1, m_1] \oplus [p_1, q_1] = [n_2, m_2] \oplus [p_2, q_2]$

$\Leftrightarrow [n_1q_1 + m_1p_1, m_1q_1] = [n_2q_2 + m_2p_2, m_2q_2]$

$\Leftrightarrow (n_1q_1 + m_1p_1)m_2q_2 = m_1q_1(n_2q_2 + m_2p_2)$

$\Leftrightarrow n_1q_1m_2q_2 + m_1p_1m_2q_2 = m_1q_1n_2q_2 + m_1q_1m_2p_2$

$\Leftrightarrow m_1n_2q_1q_2 + p_2q_1m_1m_2 = m_1n_2q_1q_2 + p_2q_1m_1m_2$ (since $n_1m_2 = m_1n_2$, $p_1q_2 = p_2q_1$)

But this is a tautology!

Hence, $\oplus$ is well defined.

Q.E.D

Theorem: Properties of addition on $\mathbb{Q}$

$\forall$ [n, m], [p, q], [k, l]$\in\mathbb{Q}$, we have

$A_{\mathbb{Q}}$(i) [n, m] $\oplus$ [p, q] = [p, q] $\oplus$ [n, m]

[n, m] $\oplus$ [p, q] = [nq + mp, mq]

$= [pm + qn, qm]$
$= [p, q] \oplus [n, m]$

$A_{\mathbb{Q}}$(ii) $([n, m] \oplus [p, q]) \oplus [k, l] = [n, m] \oplus ([p, q] \oplus [k, l])$

$$\begin{aligned}([n, m] \oplus [p, q]) \oplus [k, l] &= [nq + mp, mq] \oplus [k, l]\\ &= [(nq + mp)l + (mq)k, (mq)l]\\ &= [nql + mpl + mqk, mql]\\ &= [n(ql) + m(pl + qk), m(ql)]\\ &= [n, m] \oplus ([p, q] \oplus [k, l])\end{aligned}$$

$A_{\mathbb{Q}}$(iii) The identity element exists and is given by [0, 1]

$$\begin{aligned}[m, n] \oplus [0, 1] &= [m1 + n0, n1]\\ &= [m, n]\\ &= [0, 1] \oplus [m, n] \text{ (by } A_{\mathbb{Q}(i)})\end{aligned}$$

$A_{\mathbb{Q}}$(iv) For any [n, m], its $\oplus$-inverse exists and is given by [-n, m]

$$\begin{aligned}[n, m] \oplus [-n, m] &= [nm + m(-n), mm]\\ &= [nm - nm, mm]\\ &= [0, mm]\\ &= [0, 1]\\ &= [-n, m] \oplus [n, m] \text{ (by } A_{\mathbb{Q}(i)})\end{aligned}$$

Q.E.D

Hence, we have shown that $(\mathbb{Q},\oplus)$ is a commutative group.

Theorem: Multiplication on $\mathbb{Q}$

∃ a well-defined binary operation, $\odot$, on $\mathbb{Q}$ given by

$[n, m] \odot [p, q] = [np, mq]$

Let $[n_1, m_1] = [n_2, m_2]$ and $[p_1, q_1] = [p_2, q_2]$ where $m_1, m_2, q_1, q_2 \neq 0$. Then $n_1m_2 = m_1n_2$ and $p_1q_2 = p_2q_1$. Thus,

$[n_1, m_1] \odot [p_1, q_1] = [n_2, m_2] \odot [p_2, q_2]$
$\Leftrightarrow [n_1p_1, m_1q_1] = [n_2p_2, m_2q_2]$
$\Leftrightarrow (n_1p_1)(m_2 q_2) = (m_1q_1)(n_2 p_2)$
$\Leftrightarrow (n_1m_2)(p_1 q_2) = (m_1n_2)(p_2 q_1)$
$\Leftrightarrow (n_1m_2)(p_1 q_2) = (n_1m_2)(p_1 q_2)$ (since $n_1m_2 = m_1n_2$ and $p_1p_2 = p_2q_1$)

But this is a tautology!

Hence, $\odot$ is well defined.

Q.E.D

Theorem: Properties of Multiplication on $\mathbb{Q}$

∀ [n, m], [p, q], [k, l] ∈ $\mathbb{Q}$, we have

$M_{\mathbb{Q}}$(i) $[n, m] \odot [p, q] = [p, q] \odot [n, m]$

$$\begin{aligned}[n, m] \odot [p, q] &= [np, mq]\\ &= [pn, qm]\\ &= [p, q] \odot [n, m]\end{aligned}$$

$M_{\mathbb{Q}}$(ii) $([n, m] \odot [p, q]) \odot [k, l] = [n, m] \odot ([p, q] \odot [k, l])$

$$\begin{aligned}([n, m] \odot [p, q]) \odot [k, l] &= [np, mq] \odot [k, l] \\ &= [(np)k, (mq)l] \\ &= [n(pk), m(ql)] \\ &= [n, m] \odot ([p, q] \odot [k, l])\end{aligned}$$

$M_{\mathbb{Q}}$(iii) The identity element exists and is given by [1, 1].

$$\begin{aligned}[n, m] \odot [1, 1] &= [n1, m1] \\ &= [n, m] \\ &= [1, 1] \odot [n, m] \text{ (by } M_{\mathbb{Q}}\text{(i))}\end{aligned}$$

$M_{\mathbb{Q}}$(iv) For any element [n, m], [n, m] ≠ [0, 1], its ⊙-inverse exists and is given by [m, n].

$$\begin{aligned}[n, m] \odot [m, n] &= [nm, mn] \\ &= [nm(1), nm(1)] \\ &= [1, 1] \qquad (nm \neq 0 \text{ as } n, m \neq 0) \\ &= [m, n] \odot [n, m] \text{ (by } M_{\mathbb{Q}}\text{(i))}\end{aligned}$$

$M_{\mathbb{Q}}$(v) $[n, m] \odot ([p, q] \oplus [k, l]) = ([n, m] \odot [p, q]) \oplus ([n, m] \odot [k, l])$

$$\begin{aligned}[n, m] \odot ([p, q] \oplus [k, l]) &= [n, m] \odot [pl + qk, ql] \\ &= [n(pl + qk), m(ql)] \\ &= [npl + nqk, mql]\end{aligned}$$

$$\begin{aligned}([n, m] \odot [p, q]) \oplus ([n, m] \odot [k, l]) &= [np, mq] \oplus [nk, ml] \\ &= [npml + mqnk, mqml] \\ &= [m(npl + nqk), mmql] \\ &= [npl + nqk, mql] \qquad (\text{since } m \neq 0) \\ &= [n, m] \odot ([p, q] \oplus [k, l])\end{aligned}$$

Q.E.D

In fact, we have managed to show that ($\mathbb{Q}$/[0,1], ⊙) is a commutative group also. Since the distributive law also holds, we see that ($\mathbb{Q}$,⊕,⊙) is actually a field. Our job now is to order this field, as described in the following section.

Order on $\mathbb{Q}$

To define an appropriate order, the main job is to identify the subset of $\mathbb{Q}$ that will serve as the set of positive elements. Informally, this means that we have to consider the signs of the denominator and numerator of the fraction, and choose all those that will give a net positive sign. The following theorem tells us that such a way of getting the positive elements is actually technically possible and well-defined in our framework.

Theorem:

The subset $P_{\mathbb{Q}}$ of $\mathbb{Q}$ defined by

$P_{\mathbb{Q}} = \{[m,n] \in \mathbb{Q} \mid m, n>0 \text{ or } m, n <0\}$
is a well-defined set.

To show that $P_{\mathbb{Q}}$ is well defined, we need to show that any [m,n] cannot be both in and out of the set. Hence, let $[m_1,n_1]= [m_2,n_2]$ and suppose $[m_1,n_1]\in P_{\mathbb{Q}}$. Then $m_1n_2=m_2n_1$. Either

(a) $m_1,n_1>0$

(i) $n_2>0$

Then $m_2n_1 =m_1n_2>0$. Since $n_1>0$, we must have $m_2>0$, i.e $[m_2,n_2] \in P_{\mathbb{Q}}$.

(ii) $n_2<0$

Then $m_2n_1 =m_1n_2<0$. Since $n_1>0$, we must have $m_2<0$, i.e $[m_2,n_2] \in P_{\mathbb{Q}}$.

(b) $m_1,n_1<0$

(i) $n_2>0$

Then $m_2n_1 =m_1n_2<0$. Since $n_1<0$, we must have $m_2>0$, i.e $[m_2,n_2] \in P_{\mathbb{Q}}$.

(ii) $n_2<0$

Then $m_2n_1 =m_1n_2>0$. Since $n_1<0$, we must have $m_2<0$, i.e $[m_2,n_2] \in P_{\mathbb{Q}}$.

Hence, $P_{\mathbb{Q}}$ is a well defined subset of $\mathbb{Q}$.

Q.E.D

The following theorem tells us that $P_{\mathbb{Q}}$ is indeed the set of positive elements in $\mathbb{Q}$ since it satisfy the general criteria of a positive set in a field.

Theorem:

The set $P_{\mathbb{Q}}$ is closed under $\oplus$ and $\odot$ and for every $[m, n]\in \mathbb{Q}$, one and only one of the following is true: $[m, n] = [0, 1]$, $[m, n]\in P_{\mathbb{Q}}$, $[-m, n]\in P_{\mathbb{Q}}$.

Take $[m_1, n_1], [m_2, n_2]\in P_{\mathbb{Q}}$. We consider 4 cases:

(i) $m_1, n_1 > 0, m_2, n_2 > 0$

Then $m_1m_2, m_1n_2, n_1m_2, n_1n_2 > 0$. This means $m_1n_2 + n_1m_2, n_1n_2 > 0$ so that $[m_1, n_1] \oplus [m_2, n_2]\in P_{\mathbb{Q}}$. Also, $m_1m_2, n_1n_2 > 0$ so that $[m_1, n_1] \odot [m_2, n_2]\in P_{\mathbb{Q}}$.

(ii) $m_1, n_1 > 0, m_2, n_2 < 0$

Then $m_1m_2, n_1n_2, m_1n_2, n_1m_2 < 0$. This means $m_1n_2 + n_1m_2, n_1n_2 < 0$ so that $[m_1, n_1] \oplus [m_2, n_2]\in P_{\mathbb{Q}}$. Also, $m_1m_2, n_1n_2 < 0$ so that $[m_1, n_1] \odot [m_2, n_2]\in P_{\mathbb{Q}}$.

(iii) $m_1, n_1 < 0, m_2, n_2 > 0$

By symmetry (due to commutativity), this case is true by (ii)

(iv) $m_1, n_1 < 0, m_2, n_2 < 0$

Then $m_1m_2, m_1n_2, n_1m_2, n_1n_2 > 0$. This means $m_1n_2 + n_1m_2, n_1n_2 > 0$ so that $[m_1, n_1] \oplus [m_2, n_2]\in P_{\mathbb{Q}}$. Also, $m_1m_2, n_1n_2 > 0$ so that $[m_1, n_1] \odot [m_2, n_2]\in P_{\mathbb{Q}}$ also.

Hence, $P_{\mathbb{Q}}$ is closed under $\oplus$ and $\odot$.

Take any $[m, n]\in \mathbb{Q}$.

First, observe that $[0, 1]\notin P_{\mathbb{Q}}$ since $0 > 0$ is not true. Hence, we also cannot have $[m,n], [-m, n]\in P_{\mathbb{Q}}$ since under closure of $\oplus$, we would have $[0, 1]\in P_{\mathbb{Q}}$. Since $[0,1]=[-0,1]$, we have shown that at most one of the 3 cases is true. Now, one of the following 3 cases must be true:

(i) $m = 0$

Then $[m, n] = [0, 1]$

(ii) $m > 0$ (i.e. $-m < 0$)

(a) $n > 0$

Hence, $[m, n] \in P_{\mathbb{Q}}$.

(b) $n < 0$

Hence, $[-m, n] \in P_{\mathbb{Q}}$.

(iii) $m < 0$ (i.e. $-m > 0$)

(a) $n > 0$

Hence $[-m, n] \in P_{\mathbb{Q}}$.

(b) $n < 0$

Hence $[m, n] \in P_{\mathbb{Q}}$.

Hence, one and only one of the 3 cases is true.

Q.E.D

We can now make our fractional system an ordered field by mean of the following definition:

Defn: For any $x, y \in \mathbb{Q}$, we say x is greater than y and we write $x \succ y$ if $x \oplus (-y) \in P_{\mathbb{Q}}$. We write $x \succcurlyeq y$ if $x \succ y$ or $x = y$.

Hence, $(\mathbb{Q}, \oplus, \odot, \succ)$ is an ordered field. By now, the reader should have caught on to the rhythm of our construction process and anticipate that our next endeavor is to define a general fractional system. We call it a field of rationals.

The Field Of Rationals

If one looks through the defining properties of a field, one will realize that they are actually fundamental properties that one would expect of the intuitive fractions. Hence, a system of rationals must at least be an ordered field. It should also contain a copy of the integer system. Furthermore, its elements are supposed to be fractions so it should always be possible for one to rewrite it as one integer 'over' another. The following definition sums up our intuition:

Defn: An ordered field $(F, \oplus, \odot, \succ)$ is called a field of rationals if $\exists$ an ordered subdomain $(F_{\mathbb{Z}}, \oplus, \odot, \succ)$ such that

(i) $(F_{\mathbb{Z}}, \oplus, \odot, \succ) \simeq (\mathbb{Z}, +, ., >)$

(ii) For every $x \in F$, $\exists$ $y, z \in F_{\mathbb{Z}}$ s.t $x = y^{-1} \odot z$

We will now show that our Fractional System is actually a Field Of Rationals. We will also show that any two Fields Of Rationals will be isomorphic, and hence there is essentially only one Field Of Rationals.

Theorem:

Fields of rationals exists and is unique.

First, we claim that $(\mathbb{Q}, \oplus, \odot, \succ)$ is a Field Of Rational. Consider the subset

$\mathbb{Q}_{\mathbb{Z}} = \{[n, 1] \in \mathbb{Q} \mid n \in \mathbb{Z}\}$. Take any $[n, 1], [m, 1] \in \mathbb{Q}_{\mathbb{Z}}$,

$$\begin{aligned}[n, 1] \oplus (-[m, 1]) &= [n, 1] \oplus [-m, 1] \\ &= [n(1) + (1)(-m), (1)(1)] \\ &= [n - m, 1] \ (\in \mathbb{Q}_{\mathbb{Z}})\end{aligned}$$

$[n, 1] \odot [m, 1] = [nm, (1)(1)]$

$= [nm, 1]$ $(\in \mathbb{Q}_{\mathbb{Z}})$

Also, the $\odot$-identity $[1, 1]$ is obviously in $\mathbb{Q}_{\mathbb{Z}}$.

Hence $(\mathbb{Q}_{\mathbb{Z}}, \oplus, \odot, \succ)$ is an ordered subdomain.

(i) Consider the mapping ϕ: $\mathbb{Q}_{\mathbb{Z}} \to \mathbb{Z}$ given by

$\phi([n, 1]) = n \ \forall \ [n, 1] \in \mathbb{Q}_{\mathbb{Z}}$.

Suppose $[n, 1] = [m, 1]$. Then $n(1) = (1)m$, i.e. $\phi([n, 1]) = \phi([m, 1])$. Hence ϕ is a well-defined function.

Now, $\phi([n, 1]) = \phi([m, 1]) \Rightarrow n = m \Rightarrow [n, 1] = [m, 1]$. Hence ϕ is one-one.

Also, for any $n \in \mathbb{Z}$, take $[n, 1] \in \mathbb{Q}_{\mathbb{Z}}$ so that $\phi([n, 1]) = n$. Hence ϕ is onto.

Hence, ϕ is a bijective function.

Take any $[n, 1], [m, 1] \in \mathbb{Q}_{\mathbb{Z}}$,

$$\begin{aligned}\phi([n, 1] \oplus [m, 1]) &= \phi([n + m, 1]) \\ &= n + m \\ &= \phi([n, 1]) + \phi([m, 1])\end{aligned}$$

$$\begin{aligned}\phi([n, 1] \odot [m, 1]) &= \phi([nm, 1]) \\ &= nm \\ &= \phi([n, 1])\phi([m, 1])\end{aligned}$$

$$\begin{aligned}[n, 1] \succ [m, 1] &\Rightarrow [n, 1] \oplus [-m, 1] \in P_{\mathbb{Q}} \\ &\Rightarrow [n - m, 1] \in P_{\mathbb{Q}}\end{aligned}$$

Hence, either $(n - m, 1 < 0)$ (but this is impossible since $1 > 0$) or $(n - m, 1 > 0)$. Hence, we must have the latter and so $n > m$, i.e $\phi([n, 1]) > \phi([m, 1])$.

Hence ϕ is an isomorphism from $(\mathbb{Q}_{\mathbb{Z}}, \oplus, \odot, \succ)$ to $(\mathbb{Z}, +, ., >)$ and so $(\mathbb{Q}_{\mathbb{Z}}, \oplus, \odot, \succ) \simeq (\mathbb{Z}, +, ., >)$.

(ii) For any $[n, m] \in \mathbb{Q}$, consider the element $[m, 1], [n, 1] \in \mathbb{Q}_{\mathbb{Z}}$.

$$\begin{aligned}([m, 1])^{-1} \odot [n, 1] &= [1, m] \odot [n, 1] \\ &= [1n, m1] \\ &= [n, m]\end{aligned}$$

Hence, given any $x \in \mathbb{Q}$, $\exists$ $y, z \in \mathbb{Q}_{\mathbb{Z}}$ s.t $x = y^{-1} \odot z$.

Hence, $(\mathbb{Q}, \oplus, \odot, \succ)$ is a Field Of Rationals and so Field of Rationals exist.

Now, let $(\mathbb{Q}', \oplus', \odot', \succ')$ be any other Field Of Rationals. Since $(\mathbb{Q}_{\mathbb{Z}}, \oplus, \odot, \succ) \simeq (\mathbb{Z}, +, ., >) \simeq (\mathbb{Q}_{\mathbb{Z}}', \oplus', \odot', \succ')$, $\exists$ an isomorphism ϕ: $\mathbb{Q}_{\mathbb{Z}} \to \mathbb{Q}_{\mathbb{Z}}'$. Define the mapping ψ: $\mathbb{Q} \to \mathbb{Q}'$ by

$\psi(a) = (\phi(b))^{-1} \odot' \phi(c) \ \forall \ a \in \mathbb{Q}$, where $a = b^{-1} \odot c$ for some $b, c \in \mathbb{Q}_{\mathbb{Z}}$.

Let $a_1 = b_1^{-1} \odot c_1 = b_2^{-1} \odot c_2 = a_2$ where $b_1, b_2, c_1, c_2 \in \mathbb{Q}_{\mathbb{Z}}$.

Then

$$\begin{aligned}&b_1^{-1} \odot c_1 = b_2^{-1} \odot c_2 \\ &\Rightarrow b_2 \odot c_1 = b_1 \odot c_2 \\ &\Rightarrow \phi(b_2 \odot c_1) = \phi(b_1 \odot c_2) \\ &\Rightarrow \phi(b_2) \odot' \phi(c_1) = \phi(b_1) \odot' \phi(c_2)\end{aligned}$$

$\Rightarrow (\phi(b_1))^{-1} \odot' \phi(c_1) = (\phi(b_2))^{-1} \odot' \phi(c_2)$

$\Rightarrow \psi(a_1) = \psi(a_2)$

Hence, ψ is a well-defined function.

Now, let $\psi(a_1) = \psi(a_2)$ where $a_1 = b_1^{-1}\odot c_1$, $a_2 = b_2^{-1}\odot c_2$ for some $b_1, b_2, c_1, c_2\in \mathbb{Q}_{\mathbb{Z}}$. Then

$(\phi(b_1))^{-1} \odot' \phi(c_1) = (\phi(b_2))^{-1} \odot' \phi(c_2)$

$\Rightarrow \phi(b_2) \odot' \phi(c_1) = \phi(b_1) \odot' \phi(c_2)$

$\Rightarrow \phi(b_2\odot c_1) = \phi(b_1\odot c_2)$

$\Rightarrow b_2\odot c_1 = b_1\odot c_2$ (since ϕ is one-one)

$\Rightarrow b_1^{-1}\odot c_1 = b_2^{-1}\odot c_2$

$\Rightarrow a_1 = a_2$

Hence ψ is one-one.

Take any $a'\in \mathbb{Q}'$. $\exists$ $b', c'\in \mathbb{Q}_{\mathbb{Z}}'$ s.t $a' = b'^{-1} \odot' c'$. Since ϕ is onto $\mathbb{Q}_{\mathbb{Z}}'$, $\exists$ $b, c\in \mathbb{Q}_{\mathbb{Z}}$ s.t $\phi(b) = b'$, $\phi(c) =c'$.

Take the element $a = b^{-1}\odot c$ in $\mathbb{Q}$.Then $\psi(a) = (\phi(b))^{-1} \odot' \phi(c) = b'^{-1} \odot' c' = a'$ and so ψ is onto $\mathbb{Q}'$.

Hence, ψ is a bijective function.

Take any $a_1,a_2\in \mathbb{Q}$ where $a_1 = b_1^{-1}\odot c_1$, $a_2 = b_2^{-1}\odot c_2$ for some $b_1, b_2, c_1, c_2\in \mathbb{Q}_{\mathbb{Z}}$.

$\psi(a_1\odot a_2)$

$= \psi((b_1^{-1}\odot c_1) \odot (b_2^{-1}\odot c_2))$

$= \psi((b_2^{-1}\odot b_1^{-1}) \odot (c_1\odot c_2))$

$= \psi((b_1\odot b_2)^{-1} \odot (c_1\odot c_2))$

$= (\phi(b_1\odot b_2))^{-1} \odot' \phi(c_1\odot c_2)$

$= (\phi(b_1)\odot'\phi(b_2))^{-1} \odot' (\phi(c_1)\odot'\phi(c_2))$

$= ((\phi(b_2))^{-1}\odot'(\phi(b_1))^{-1}) \odot' (\phi(c_1)\odot'\phi(c_2))$

$= ((\phi(b_1))^{-1}\odot'\phi(c_1)) \odot' ((\phi(b_2))^{-1}\odot'\phi(c_2))$

$= \psi(a_1) \odot' \psi(a_2)$

$\psi(a_1\oplus a_2)$

$= \psi((b_1^{-1}\odot c_1) \oplus (b_2^{-1}\odot c_2))$

$= \psi((b_1^{-1}\odot b_2^{-1}) \odot((b_2\odot c_1) \oplus (b_1\odot c_2)))$

$= \psi((b_2\odot b_1)^{-1} \odot((b_2\odot c_1) \oplus (b_1\odot c_2)))$

$= (\phi(b_2\odot b_1))^{-1} \odot' \phi((b_2\odot c_1) \oplus (b_1\odot c_2))$

$= (\phi(b_2)\odot'\phi(b_1))^{-1} \odot' (\phi(b_2\odot c_1) \oplus' \phi(b_1\odot c_2))$

$= ((\phi(b_1))^{-1}\odot'(\phi(b_2))^{-1}) \odot' ((\phi(b_2)\odot'\phi(c_1)) \oplus'(\phi(b_1)\odot'\phi(c_2)))$

$= (((\phi(b_1))^{-1}\odot'(\phi(b_2))^{-1})\odot' (\phi(b_2)\odot'\phi(c_1)))\oplus'((\phi(b_1))^{-1}\odot'(\phi(b_2))^{-1})\odot'(\phi(b_1)\odot'\phi(c_2)))$

$= ((\phi(b_1))^{-1}\odot'\phi(c_1)) \oplus' ((\phi(b_2))^{-1}\odot'\phi(c_2))$

$= \psi(a_1) \oplus' \psi(a_2)$

$a_1 \succ a_2 \Rightarrow b_1^{-1}\odot c_1 \succ b_2^{-1}\odot c_2$

We consider 2 cases:

a) $b_1,b_2 \succ 0$ or $b_1,b_2 \prec 0$, hence $b_1 \odot b_2 \succ 0$

First note that this means $\phi(b_1),\phi(b_2) \succ' 0'$ or $\phi(b_1),\phi(b_2) \prec' 0'$ also, hence $(\phi(b_1))^{-1} \odot' (\phi(b_2))^{-1} \succ' 0'$

Then

$b_1^{-1} \odot c_1 \succ b_2^{-1} \odot c_2$

$\Rightarrow b_2 \odot c_1 \succ b_1 \odot c_2$

$\Rightarrow \phi(b_2 \odot c_1) \succ' \phi(b_1 \odot c_2)$

$\Rightarrow \phi(b_2) \odot' \phi(c_1) \succ' \phi(b_1) \odot' \phi(c_2)$

$\Rightarrow (\phi(b_1))^{-1} \odot' \phi(c_1) \succ' (\phi(b_2))^{-1} \odot' \phi(c_2)$

$\Rightarrow \psi(a_1) \succ' \psi(a_2)$

b) $(b_1 \succ 0, b_2 \prec 0)$ or $(b_2 \succ 0, b_1 \prec 0)$, hence $b_1 \odot b_2 \prec 0$

First note that this means $(\phi(b_1) \succ' 0', \phi(b_2) \prec' 0')$ or $(\phi(b_2) \succ' 0', \phi(b_1) \prec' 0')$ also, hence $(\phi(b_1))^{-1} \odot' (\phi(b_2))^{-1} \prec' 0'$

Then

$b_1^{-1} \odot c_1 \succ b_2^{-1} \odot c_2$

$\Rightarrow b_2 \odot c_1 \prec b_1 \odot c_2$

$\Rightarrow \phi(b_2 \odot c_1) \prec' \phi(b_1 \odot c_2)$

$\Rightarrow \phi(b_2) \odot' \phi(c_1) \prec' \phi(b_1) \odot' \phi(c_2)$

$\Rightarrow (\phi(b_1))^{-1} \odot' \phi(c_1) \succ' (\phi(b_2))^{-1} \odot' \phi(c_2)$

$\Rightarrow \psi(a_1) \succ' \psi(a_2)$

Hence, $a_1 \succ a_2 \Rightarrow \psi(a_1) \succ' \psi(a_2)$

Hence, ψ is an isomorphism from $(\mathbb{Q}, \oplus, \odot, \succ)$ to $(\mathbb{Q}', \oplus', \odot', \succ')$ and so

$(\mathbb{Q}, \oplus, \odot, \succ) \simeq (\mathbb{Q}', \oplus', \odot', \succ')$

Hence, Field Of Rationals exist and they are unique.

Q.E.D

As we have done in Chapter 2, we will now abandon our specific Fractional System and speak only of the Field Of Rationals, denoted by $(\mathbb{Q}, +, ., >)$. The Natural system and the Integer system embedded within the Field Of Rationals will be respectively denoted by $(\mathbb{N}, +, ., >)$ and $(\mathbb{Z}, +, ., >)$. The next section will reveal to us some special properties of the Field Of Rationals, and we will see that this new system is actually quite different from the previous two systems.

Special Properties of $\mathbb{Q}$

This section will show us properties of $\mathbb{Q}$ that we would expect of a system that is supposed to model our intuitive fractions. Note that most proofs unique to $\mathbb{Q}$ have to make use of (ii) of the definintion of the field of rationals. This is not surprising, for that is essentially the unique characteristic of $\mathbb{Q}$. Hence, when we say in a proof that we can always write a rational r as n/m for some integer n, m, we are actually ultilizing this property. Sometime, we even claim that n, m are natural numbers but that will be mostly due to ordering properties that we have ascribed to r in that proof.

Hence, the author would like to take this chance to remind the reader again that nothing familar has been or will be assumed. We will now prove first that the Archimedean Property holds for $\mathbb{Q}$ also.

Theorem: Archimedean Property for $\mathbb{Q}$

For any $x, y \in \mathbb{Q}$, $x>0$, $\exists z \in \mathbb{N}$ s.t $zx > y$.

We may assume $y>0$ else just take $z=1\in \mathbb{N}$. Since $x, y>0$, we can choose $m,n,p,q\in \mathbb{N}$ s.t $x= m/n$ and $y= p/q$. Then $mq, np\in \mathbb{N}$ and by the Archimedean Property for $\mathbb{N}$, $\exists$ $z\in \mathbb{N}$ s.t

$zmq > np$

$\Rightarrow z(m/n) > p/q$ (since $1/n, 1/q >0$)

Hence, the Archimedean property for $\mathbb{Q}$ holds.

Q.E.D

Note that the special case $x=1$ tells us that given any $y\in \mathbb{Q}$, $\exists$ $z \in \mathbb{N}$ s.t $z> y$. This allows us to immediately conclude that any subset of $\mathbb{N}$ (or $\mathbb{Z}$ for that matter) that is bounded above by some rational is in fact also bounded above by some number in $\mathbb{N}$ (and hence $\mathbb{Z}$) so that we can make use of 'internal bounded properties' of such subsets. Now, we can prove that a rational is always between two consecutive integers:

Theorem:

For every rational r, there exist an unique integer n such that $n\leq r < n+1$

Let $A =\{ n\in \mathbb{Z} \mid n \leq r\}$. If $r\geq 0$, then clearly $0\in A$. If $r<0$, then $-r>0$. By the Archimedean property for $\mathbb{Q}$, $\exists$ an $n_0\in \mathbb{N}$ (and hence in $\mathbb{Z}$) s.t $n_0> -r$, i.e $r>-n_0$ and so $-n_0\in A$. Hence, A is a non-empty subset of $\mathbb{Z}$ and since it is also bounded above by some element of $\mathbb{Z}$, by order completeness of $\mathbb{Z}$, n= MaxA must exists. Hence, $n\leq r < n+1$. If another such integer $m \in\mathbb{Z}$ exists, then $m\in A$ so that $m\leq n$. But $m\leq n\leq r< m+1$. Since there are no integers strictly between m and m+1, we must have m =n and so such an integer is unique.

Q.E.D

The next theorem tells us that $\mathbb{Q}$ is not discrete by showing us that it is in fact a 'dense' system.

Theorem: Denseness of $\mathbb{Q}$

For any $x,y \in \mathbb{Q}$ with $x<y$, $\exists z \in \mathbb{Q}$ s.t $x<z<y$.

Take $z=(1/2)(x+y) \in \mathbb{Q}$.Then

$x<y \Rightarrow x+x < x+y,\ x+y<y+y$

$\Rightarrow 2x < x+y,\ x+y<2y$

$\Rightarrow x < (1/2)(x+y),\ (1/2)(x+y)<y$, i.e $x<z<y$

Q.E.D

What has this result got to do with the notion of $\mathbb{Q}$ being dense? Well, we can always repeat the above process with x and z to get a new z′. Nothing stops us from applying the process again on x and z′ and in this way, we generate an infinite number of distinct rational between x and y. Hence, $\mathbb{Q}$ is dense in the sense that between any two unequal rational, there are infinite number of distinct rational!

The next theorem tells us that $\mathbb{Q}$ is not well-ordered, which is basically a consequence of the fact that it contains a substructure that is itself not well-ordered.

Theorem:

$\mathbb{Q}$ is not well-ordered

If $\mathbb{Q}$ is well ordered, then every nonempty subset of $\mathbb{Q}$ has a minimum. But any nonempty subset of $\mathbb{Z}$ is also a nonempty subset of $\mathbb{Q}$ and hence any non-empty subset of $\mathbb{Z}$ also has a minimum and since the minimum belong to a subset of $\mathbb{Z}$, it is an element of $\mathbb{Z}$. Hence, this must contradict $\mathbb{Z}$ being not well-ordered and so $\mathbb{Q}$ cannot be well-ordered also.

Q.E.D

Inadequacy Of $\mathbb{Q}$

For most practical purposes in our daily life, the Field of Rational can be said to be more than adequate as a number system. After all, when we take a measurement with our ruler, we can read at best to the markings on the ruler and those markings are simply fractions of the length of the ruler. Even when we use an electronic calculator and obtained a result whose figures covered the whole screen, we simply round off to our desired accuracy with not much complaint. Now, when we round off something, we are simply getting a result that can be expressed as a fraction. So what exactly is wrong with the Field of Rational?

Most people's idealization of the real numbers is that they are markings on an imaginary number line. This number line is a sort of conceptual ruler that mathematicians can use to measure their abstract objects exactly. This means that the number line will always give us the exact value, and not just any approximated value, of any quantity we are measuring. Of course, some sort of standardization of the division mark should be used so that everybody's absolute value agree but that is beside the point. Now, if the Field of Rational gives us such an ideal number system, then we should be able to cover the whole of the number line with rational numbers. If this cannot be achieved, then there will be at least one point on the number line that have no markings, and what value are we going to assign an object whose length happen to hit that mark?

Let us prove the following theorem first before we continue our discussion. It will enable us to provide a 'physical' argument that the rationals cannot be our ideal number system.

Theorem:

There exists no rational r such that $r^2=2$.

Suppose that such a rational r does exist. We can then assume r>0, since if this is not so, we can then always consider –r>0. Then ∃ m, n∈ ℤ s.t r= m/n and g.c.d(m,n)=1. Then
$(m/n)^2=2$, i.e $m^2=2n^2$

This means m^2 is even and so m is even. We can then write m=2k for some k∈ ℕ and we have
$(2k)^2 = 2n^2$, i.e $2k^2 =n^2$

But this mean n^2 (and hence n) is even. In particular, 2 is a common divisor of m and n, contradicting g.c.d(m,n)=1.

Q.E.D

This is rather an interesting result and so we will digress a bit and discuss more on this result first. In a more general setting, there does not exist r∈ℚ s.t r^2 =p, where p is a prime. Before we put p into the above proof and try to see whether the whole thing still work, we postulate an informal argument that would intuitively reveal why the claim always work for prime. As usual, we consider the equation m^2=pn^2 and we count the number of primes (repetitive primes are also counted) that occur in the prime factorization of m^2 and pn^2. With the fundamental theorem of arithmetic, the number of primes on both sides must at least agree, if their product is to have any hope of being the same. But m^2 will have twice the number of primes of m, and so its number of prime is even. Similarly, n^2 has an even number of primes and with the introduction of an additional prime, p, pn^2 now has an odd number of primes and so we have our contradiction. If p is not prime, then we would not know how many primes is actually in the prime factorization of p and hence nothing can be concluded. In fact, this argument also tell us that any composite number with an odd number of prime in its prime factorization (such as 8, 30 etc) yields the same claim. We can even carry on further with this argument and see that any composite number with at least one type of prime in its prime factorization occurring an odd number of times yields the same claim. Hence, only perfect square can be the square of some rationals. But perfect square are trivially always the square of some rationals(integers in fact) and so we can roughly see that the ‘number’ of ‘holes’ in the rationals is at least as large as the number of integers that is not a perfect square.

One may wonder what the big fuss is with the above theorem. An imaginary number line is well and good for the mathematicians but the number line exist in the mind, and is not a physical object. We seek to fill up gaps in the number line, but perhaps these gaps have no physical analogy at all. In other words, one may never find something in nature that require a non- rational marking. Things in nature are always nice proportions of whole things, and one should never be too irrationally abstract and extrapolate everything in the mind to the concrete and physical...

Well, let us take a ruler and pencil and try to draw something physical then. Of course, the author would not suggest that one draws a line with a non-rational length directly with the ruler since the ruler is but rational in nature. Perhaps we can arbitrary draw a line and hope to achieve a non- rational length. But this method is silly since how can we verify that we have indeed achieved a non-rational length? Taking a leaf from history, the author would suggest that one draws two lines perpendicular to each other and each of length 1 unit long, whatever unit that your ruler possess. Join the two open ends of the lines together to get a closed triangle. Measure now the length of this new line and you will see that...well...you will not hit an exact marking so let us try another method. Flipping through some elementary book on geometry, we found that the Pythagorean's theorem (which happen to be a gemstone in measuring triangle's length) tells us that the value should be the square root of 2. In other words, the answer is a number that when squared gives 2. Some theorems in Mathematics are really annoying in the sense that they gives us result that we would rather hope not be true. In this case, the above theorem is hence annoying by definition since it tells us that the length that we have just drawn cannot have any rational numbers ascribed to it.

Well, we have drawn a triangle, a physical object if we may add, that has a length that cannot be measured. For readers whose intuition tells them that a triangle drawn physically by a flesh and blood human on a piece of solid paper with a metal ruler and carbon pencil remains in the domain of the imagination can stop here now and we are done with the construction. But for interested readers who believe that there are some numbers out there which is not rational, the author invites them to read on. For the rest of the construction, we will be imagining a number line and our informal discussion would always be based on how an ideal number line should behave. We will now place first all the rational numbers onto the number line and we prove two theorems that each gives us a technical motivation to construct the real number system.

First of all, the following theorem tells us that $\mathbb{Q}$ is not order complete. We will comment on what this means in our number line analogy immediately after the proof.

<u>Theorem:</u>

$\mathbb{Q}$ does not have the least upper bound property. In particular, $\mathbb{Q}$ is not order complete.

Consider the set $A = \{r \in \mathbb{Q} \mid r > 0 \text{ and } r^2 < 2\}$. Clearly $4/3 \in A$ so A is non-empty. Also, A is bounded above by 2 since $r > 2 \Rightarrow r^2 > 4 \geq 2$, i.e. $r \in A \Rightarrow r \leq 2$. Now, suppose that u = SupA exists. Note that $u \geq 4/3 > 1 > 0$ and we consider 3 cases:

(i) $u^2 = 2$

This has been shown to be impossible.

(ii) $u^2 < 2$ (i.e $u \in A$)

For $n \in \mathbb{N}$,

$$(u + 1/n)^2 < 2 \Leftrightarrow u^2 + 2(u)(1/n) + (1/n)^2 < 2$$
$$\Leftrightarrow 2(u)(1/n) + (1/n)^2 < 2 - u^2$$

Since $u \leq 2$(as 2 is an upper bound), $(1/n)^2 \leq 1/n$,

we have $2(u)(1/n) + (1/n)^2 \leq 2(2)(1/n) + 1/n$
$= 5/n$

Since $5, 2 - u^2 > 0$, by the Archimedean property of $\mathbb{Q}$, $\exists\, n_0 \in \mathbb{N}$ s.t $n_0(2- u^2)>5$, i.e. $2(u)(1/ n_0) + (1/ n_0)^2 \leq 5/ n_0 < 2 - u^2$. In other word, $(u + 1/ n_0)^2 < 2$ and so $u + 1/ n_0 \in A$. This contradicts u being the suprema of A since $u < u + 1/ n_0$. Hence, this is not possible.

(iii) $u^2 > 2$

For $n \in \mathbb{N}$, $u - 1/n$ cannot be an upper bound for A and so $\exists\, r \in A$ s.t $r > u - 1/n$. Note that $u-1/n > 0$.

Then

$(u - 1/n)^2 < r^2 < 2$

Also,

$(u - 1/n)^2 = u^2 - 2(u)(1/n) + (1/n)^2$

$> u^2 - 2(u)(1/n)$

Now, $2u$, $u^2 - 2 > 0$ so by the Archimedean property for $\mathbb{Q}$, $\exists\, n_0 \in \mathbb{N}$ s.t

$n_0(u^2 - 2) > 2u \Leftrightarrow u^2 - 2 > 2u(1/n_0)$

$\Leftrightarrow u^2 - 2u(1/n_0) > 2$

But this means

$2 > (u - 1/n_0)^2 > u^2 - 2(u)(1/n_0) > 2$, a contradiction!

Hence, this is not possible.

Hence, SupA cannot exist and so $\mathbb{Q}$ does not have the least upper bound property, i.e. it is not order complete.

Q.E.D

Now, for any non-empty subset, A of the rationals that is bounded above by some rational r, let us place an 'infinitely thin' wall at the point r. Let us slowly push the wall to the left until we reach the point where any more movement to the left would cause some element of A to be on the right side of the wall. The above theorem essentially tells us that there is at least one non-empty subset that is bounded above in which such a thing cannot be achieved. This seems strange for a number line that is supposed to be 'continuous'. One pausible explanation is that the rationals do not cover the whole of the ideal number line, and since our wall is restricted to float on rationals, then obviously, there will be sets with non-rational point as the suprema point which our wall cannot reach. Dedekind's approach essentially seeks to fill up such holes by trying to extend the Field of Rationals into an order complete field and we will do this in the next chapter.

Consider now the following theorem which tells us that $\mathbb{Q}$ is also not Cauchy Complete:

Theorem:

$\mathbb{Q}$ is not Cauchy Complete

Consider the following sequence (r_n) defined as such:

$r_1 = 3/2$

$r_{n+1} = r_n/2 + 1/r_n$

We first make a few observations:

(i) Let $P = \{n \in \mathbb{N} \mid r_n > 0\}$. Obviously, $3/2 > 0$ and so $1 \in P$. Suppose $n \in P$. Then $r_n > 0$, i.e. $r_n/2$, $1/r_n > 0$ and so $r_{n+1} = r_n/2 + 1/r_n > 0$. Hence $n + 1 \in P$ whenever $n \in P$ and by N(v), $P = \mathbb{N}$.

Hence $r_n > 0\ \forall\, n \in \mathbb{N}$.

(ii) Let $P = \{n \in \mathbb{N} \mid r_n^2 > 2\}$. Obviously, $(3/2)^2 = 9/4 > 2$ and so $1 \in P$.
Suppose $n \in P$. Then $r_n^2 - 2 > 0$, i.e. $(r_n^2 - 2)^2 > 0$. Hence

$0 < (r_n^2 - 2)^2$

$= r_n^4 - 4r_n^2 + 4$

$= r_n^2 (r_n^2 - 4 + 4/r_n^2) \qquad (\because\ r_n^2 > 0 \text{ by (i)})$

Hence, we must have $r_n^2 - 4 + 4/r_n^2 > 0$. But

$r_{n+1}^2 - 2 = (r_n/2 + 1/r_n)^2 - 2$

$= r_n^2/4 + 1 + 1/r_n^2 - 2$

$= r_n^2/4 + 1/r_n^2 - 1$

$= (1/4)(r_n^2 + 4/r_n^2 - 4)$

> 0 (Since $r_n^2 + 4/r_n^2 - 4$, $1/4 > 0$)

i.e. $r_{n+1}^2 > 2$

Hence, $n + 1 \in P$ whenever $n \in P$ and by N(v), $P = \mathbb{N}$.

Hence $r_n^2 > 2\ \forall\ n \in \mathbb{N}$.

Also,

$$
\begin{aligned}
r_{n+1}^2 - 2 &= (1/4)(r_n^2 + 4/r_n^2 - 4) \\
&= (r_n^4 + 4 - 4r_n^2)/ (4r_n^2) \\
&= (r_n^2 - 2)^2/ (4r_n^2) \\
&< (1/8)(r_n^2 - 2)^2 \qquad (\because\ r_n^2 > 2)
\end{aligned}
$$

Now, by recurring the above relation, we obtain

$$
\begin{aligned}
r_{n+1}^2 - 2 &< (1/8)(r_n^2 - 2)^2 \\
&< (1/8)((1/8)(r_{n-1}^2 - 2)^2)^2 \\
&= (1/8)^3(r_{n-1}^2 - 2)^4 \\
&< (1/8)^3 ((1/8)(r_{n-2}^2 - 2)^2)^4 \\
&= (1/8)^7 (r_{n-2}^2 - 2)^8 \\
&\ \vdots \\
&< (1/8)^m (r_1^2 - 2)^{m'} \quad \text{where } m = \Sigma 2^i \text{, the summation being taken from } 0 \le i \le n-1 \\
&\qquad\qquad m' = 2^n
\end{aligned}
$$

Now, first note that both $m, m' \in \mathbb{N}$. Also, $r_1^2 - 2 = 9/4 - 2 = 1/4 < 1$. This mean we always have $0 < (r_1^2 - 2)^{m'} < 1$. Hence, we have $r_{n+1}^2 - 2 < 1/8^m$

Now let any $\varepsilon > 0$ be given. By Archimedean property of $\mathbb{Q}$, $\exists\ k' \in \mathbb{N}$ s.t $1 < k'\varepsilon$. By Archimedean property (exponentiation version) of $\mathbb{N}$, $\exists\ k \in \mathbb{N}$ s.t $k' < 8^k$, i.e $1 < \varepsilon 8^k$. Hence,

$$
\begin{aligned}
|\, r_{n+1}^2 - 2 \,| &= r_{n+1}^2 - 2 \qquad (\because\ r_{n+1}^2 > 2) \\
&< 1/8^m \\
&< 1/8^{(n-1)} \qquad (\because\ m \ge n-1) \\
&< \varepsilon \qquad \forall\ n \ge k+1
\end{aligned}
$$

Hence, we have $(r_{n+1}^2) \to 2$, i.e $(r_n^2) \to 2$. Hence, (r_n^2) must be a Cauchy sequence as it is convergent.

Now, since $r_n > 0$ and $r_n^2 > 2$, we must have $r_n > 1$, else $r_n^2 \le 1$, contradicting $r_n^2 > 2$.

Let any $\varepsilon > 0$ be given. Then $\exists\ k \in \mathbb{N}$ s.t

$|\, r_n^2 - r_m^2 | < \varepsilon\ \ \forall\ n, m \ge k$

But

$$
\begin{aligned}
|\, r_n - r_m| &< |\, r_n - r_m|(r_n + r_m) \quad (\because\ r_n + r_m > 1) \\
&= |\, r_n - r_m||\, r_n + r_m| \\
&= |\, r_n^2 - r_m^2| \\
&< \varepsilon \qquad \forall\ n, m \ge k
\end{aligned}
$$

Hence, (r_n) is also Cauchy. If the limit of (r_n), r, exist, then since $r_n > 1\ \forall\ n \in \mathbb{N}$, we must have $r \ge 1$, i.e $r \ne 0$. Hence, $(1/r_n)$ is also convergent and we have

$$
\begin{aligned}
r = \lim r_{n+1} &= \lim (r_n/2 + 1/r_n) \\
&= (1/2)\lim r_n + \lim 1/r_n \\
&= r/2 + 1/r
\end{aligned}
$$

i.e $r/2 = 1/r$ which means $r^2 = 2$. But we have shown that such an r cannot be in $\mathbb{Q}$ and so (r_n) cannot be convergent.

Hence, $\mathbb{Q}$ is not Cauchy complete.

Q.E.D

Intuitively, this theorem is also very strange since we would expect numbers that are squeezed very tight to one another to cluster around some fixed point. Again, we can explain this if we believe that the number line is full of holes when we just consider the rational points and that Cauchy sequences of rationals really do converge to some point on the line, just that the point may happen to be a 'hole' which resides no rationals. This provides us with another approach to create the real number system. Cantor's approach essentially consider all rational Cauchy sequences and try to locate all the 'holes' by identifying them with the 'supposed' convergence point of such sequences.

The next chapter will demonstrate both these approaches in creating a real number system. The natural questions arises: Will Dedekind's approach manage to fill up all the holes in the number line by considering suprema of rational subsets that is bounded above? Can Cantor's approach patch up the holes with the convergence points of his Cauchy sequences of rationals? In other words, will these two approaches eventually leads to a common real number system?

We shall find out.

End Of Chapter 3

CHAPTER 4: THE REAL NUMBER SYSTEM

Introduction

In the previous chapter, we have demonstrated that the Field of Rationals is not really the ideal candidate for the post of the real number system. The natural question arises: What actually is the real number system then? Peano's axioms gives us a description of the natural number system that most of us will take at face value. After we have used his axioms to built up a concrete natural system, nobody should have any more difficulty accepting that our final product really do models the natural numbers. As for the definition of the Integer System and Field of Rationals, they should pose no problem to the intuition also. Both can be aptly described by elements from the preceding system. But how does one describe a real number from the rationals?

The reader should not fret if no immediate description comes to mind. For a long period in the history of mathematics, it was thought that the rationals are the only 'real numbers' existing. The reason for this is obvious. There are no 'natural' way to conceptualize a non-rational number from the rationals. We subtract in the natural system that is not closed under subtraction to generate the integers. The same trick was repeated with division in the integer system to obtain the rationals. Now, we possessed a system that is closed under all 4 natural operations (except for division by zero, of course) so what else can we attempt? Perhaps we are desperate enough to try defining division by zero to get a really 'closed-division' system, but that approach would most probably gives us only two more extra 'infinitely large' elements (positive and negative) and that does not really answer our dilemma with the triangle. So what else can we do?

Since our daily intuition does not help us in this matter, let us then appeal to higher authority and relies on the intuition of two great mathematicians, Richard Dedekind(1831-1916) and Georg Cantor(1845-1918). This chapter will see the construction of two type of real number systems, the Dedekind Real Number System and Cantor Real Number System. The former aims at order completeness, while the latter has its goal set on Cauchy completeness. After the erection of both structures, we will attempt to compare them and pick the best one for our real number system.

CHAPTER 4.1: DEDEKIND REAL NUMBER SYSTEM

The Dedekind's Cut

Defn: A subset, α, of $\mathbb{Q}$ is called a cut if it has the following properties:

$\mathbb{R}$(i) $\alpha \neq \varnothing, \alpha \neq \mathbb{Q}$

$\mathbb{R}$(ii) For every $r \in \alpha$ and $s \in \mathbb{Q} \backslash \alpha$, $r < s$

$\mathbb{R}$(iii) Maxα does not exist.

Let us have an informal discussion on this definition. Intuitively, Dedekind viewed each point, x, on the number line as a cut that split the rationals into 2 sets. In our axiomatic setup, the cut α would represent the set of all rationals strictly before the point x. To see this, we would of course have to assume that we already know the properties of the real numbers. The definition cannot directly say that α is the set of all rationals strictly before the point x since the real numbers are as yet undefined. Suppose that we are Dedekind who is quite familiar with the properties of the real number but is trying to give an axiomatic definition from the rationals, then can we spot any immediate potential pitfall in this approach?

Now, since each cut is supposed to represent a real number, we certainly cannot allow 2 different points to generate the same cut. This worry is unfounded if we happen to talk about 2 rational points. If the rational points are unequal, then one would be strictly smaller than the other and the cut generated by the smaller rational would certainly be a proper subset of the bigger one. What happen then if we chance upon two non-rational points? Since the non-rational points are actually gaps between the rationals, can it not be that two points can be placed not the same distance but each very close before a certain rational so that both points actually generate the same cut? Well, this seems possible intuitively but since we all know that the density theorem for real numbers is true, we have no worry about that either.

A final note before we start our construction. We have said that this approach is aimed at order-completeness so why are we just talking about some abstract cut of the number line? Well, each cut is actually a special subset of the rationals that is bounded above. We are using all these subsets and their 'supposed' suprema to locate all the real points.

We will now prove a fundamental theorem which will aid us immensely in the construction process. Note that we will denote the collection of all cuts by $\mathbb{R}$.

Theorem:

Let $\alpha \in \mathbb{R}$. Then for every rational $\varepsilon > 0$, $\exists\, r \in \alpha$ and $s \notin \alpha$ s.t $s - r < \varepsilon$.

Let any rational $\varepsilon > 0$ be given.

By $\mathbb{R}$(i), $\exists\, r' \in \alpha$ and $s' \notin \alpha$. By $\mathbb{R}$(ii), we then have $r' < s'$. Now, by the Archimedean property for $\mathbb{Q}$, there exist $k \in \mathbb{N}$ s.t

$(s' - r')/k < \varepsilon$

Consider the set

$A = \{ n \in \mathbb{N} \mid r' + (n/k)(s' - r') \notin \alpha \}$

Now, $k\in A$ so A is not empty. Since $\mathbb{N}$ is well-ordered, k' =MinA exist. If $k'\neq 1$, then by the defining property of A, $k'-1\notin A$. If $k'=1$, then since $r'\in\alpha$, $k'-1=0 \notin A$ also. Hence, we always have $k'-1\notin A$. Define

$r = r' + ((k'-1)/k)(s' - r') \in \alpha$

$s = r' + (k'/k)(s' - r') \qquad \notin \alpha$

Then

$s - r = (s' - r')/k < \varepsilon$.

As a corollary, given any $\varepsilon > 0$, we can always find a $r\in\alpha$ s.t $r + \varepsilon\notin\alpha$. Simply observe that $r + \varepsilon > s$ and $s\notin\alpha$. By $\mathbb{R}$(ii), $r + \varepsilon \notin \alpha$ also.

Q.E.D

Informally, this theorem in fact tells us something about the nature of the gaps in the rationals. For every non-rational points, x, on the number line, this theorem says that we can find rationals as close as we please to that point, at least in the sense of rational measurement. For example, if we want to find a rational that is at most ½ unit distant from x, then the theorem tells us there is a rational, r strictly before x such that r+1/2 is after x. Then the point x is between r and r+1/2 so it should be less than ½ unit from r. Hence, gaps between the rationals should be infinitely small and cannot be measured with any rational ruler, reinforcing our conviction that their nature are actually points.

Some Special Cuts

In this section, we will introduce two special cuts that represent significant types of real numbers. For example, each rational cut represent a rational number and the negative cut of a cut is actually the additive inverse of that cut. We postpone the introduction of the reciprocal cut since the definition of multiplication require first the concept of a set of positive real numbers which has not been developed yet.

Theorem: Rational Cuts

If $r\in\mathbb{Q}$, then the set defined by

$\alpha_r = \{x\in\mathbb{Q} \mid x < r\}$

is a cut. We call α_r a rational cut. Furthermore,

(i) $\alpha_r = \alpha_s$ ***iff*** $r = s$

(ii) α ***is a rational cut iff*** $\min(\mathbb{Q}\mid\alpha) = r$ ***exist. In that case,*** $\alpha = \alpha_r$.

Since $r\notin\alpha_r$ and $r - 1\in\alpha_r$, $\mathbb{R}$(i) is true. For any $x\in\alpha_r$ and $y\notin\alpha_r$, we have $x < r\leq y$ and so $\mathbb{R}$(ii) is true. If $\max\alpha_r$ exists, then by the density theorem for $\mathbb{Q}$, $\exists$ $x\in\mathbb{Q}$ s.t $\max\alpha_r < x < r$. This means $x\in\alpha_r$ which contradict the definition for $\mathrm{Max}\alpha_r$. Hence $\mathbb{R}$(iii) is also true.

(i) If $r = s$, then $x\in\alpha_r \Leftrightarrow x < r = s \Leftrightarrow x\in\alpha_s$.
Suppose $\alpha_r = \alpha_s$. If $r < s$, then $r\in\alpha_s$ but $r\notin\alpha_r$, a contradiction! By symmetry, $r > s$ is also not true so we must have $r = s$.

(ii) Let α_r be a rational cut. Then for any $y\in\mathbb{Q}\backslash\alpha_r$, we have $y \geq r$. Since $r\notin\alpha_r$, i.e $r\in\mathbb{Q}\backslash\alpha_r$, we have $\min(\mathbb{Q}\backslash\alpha_r) = r$. Now suppose $\min(\mathbb{Q}\backslash\alpha) = r$ exists. Then we claim $\alpha_r = \alpha$. Now,

$x\in\alpha_r \Rightarrow x < r$ $\qquad\qquad$ $x\in\alpha \Rightarrow x < r$ (since $r\in\mathbb{Q}\backslash\alpha$ and by $\mathbb{R}$(ii))

$\Rightarrow x \notin \mathbb{Q}\backslash\alpha$ (since $r = \min(\mathbb{Q}\backslash\alpha)$) $\Rightarrow x \in \alpha_r$

$\Rightarrow x \in \alpha$

Hence, $\alpha = \alpha_r$.

Q.E.D

The set of rational cuts is obviously meant to represent the rationals. Hence, we will denote the set of all rational cuts by $\mathbb{R}_{\mathbb{Q}}$.

<u>Theorem: The negative cut</u>

For any $\alpha \in \mathbb{R}$, the set defined by

$-\alpha = \{-s \in \mathbb{Q} \mid s \notin \alpha, s \neq \min(\mathbb{Q}\backslash\alpha)\}$

is also a cut. We call this the negative cut of α.

Since $\alpha \neq \mathbb{Q}$, $\exists$ $s \notin \alpha$. Then $s + 1 \notin \alpha$ and $s + 1 \neq \min(\mathbb{Q}\backslash\alpha)$. Hence, $-(s + 1) \in -\alpha$ and so $-\alpha \neq \varnothing$. Since $\alpha \neq \varnothing$, $\exists$ $s \in \alpha$. Then obviously, $-s \notin -\alpha$ and so $-\alpha \neq \mathbb{Q}$. Hence $\mathbb{R}$(i) holds.

Let $r \in -\alpha$ and $s \in \mathbb{Q}\backslash(-\alpha)$ be s.t $r \geq s$. Then $-r \leq -s$. Now, we must have $-r \notin \alpha$. Also one of the following must be true:

(i) $-s \in \alpha$

But this contradicts $\mathbb{R}$(ii) and so is impossible.

(ii) $-s = \min(\mathbb{Q}\backslash\alpha)$.

Then $-s \leq -r$, forcing $-s = -r$, i.e. $s = r$ which is absurd since $(-\alpha) \cap (\mathbb{Q}\backslash(-\alpha)) = \varnothing$.

Hence $\mathbb{R}$(ii) holds.

Suppose $\max(-\alpha)$ exists. Then $-\max(-\alpha) \notin \alpha$ and $-\max(-\alpha) \neq \min(\mathbb{Q}\backslash\alpha)$.

We consider 2 cases:

(i) $\min(\mathbb{Q}\backslash\alpha)$ does not exist

$\exists$ $s \in \mathbb{Q}\backslash\alpha$ s.t $s < -\max(-\alpha)$, else $s \geq -\max(-\alpha)$ $\forall$ $s \in \mathbb{Q}\backslash\alpha$ and since $-\max(-\alpha) \in \mathbb{Q}\backslash\alpha$, we will have $-\max(-\alpha) = \min(\mathbb{Q}\backslash\alpha)$, which contradict our assumption! Then $-s \in -\alpha$ and $-s > \max(-\alpha)$, a contradiction!

(ii) $\min(\mathbb{Q}\backslash\alpha)$ exists.

By density theorem for $\mathbb{Q}$, $\exists$ $s \in \mathbb{Q}$ s.t $\min(\mathbb{Q}\backslash\alpha) < s < -\max(-\alpha)$. As $\min(\mathbb{Q}\backslash\alpha) \in \mathbb{Q}\backslash\alpha$, we must have $s \in \mathbb{Q}\backslash\alpha$ by $\mathbb{R}$(ii). Then $-s \in -\alpha$ and $-s > \max(-\alpha)$, giving the same contradiction again.

Hence $\mathbb{R}$(iii) holds.

Hence, $-\alpha$ is also a cut.

Q.E.D

We also prove here a small result which will facilitate our algebraic manipulation later.

<u>Lemma:</u>

The negative cut of α_r is α_{-r}.

$x \in -\alpha_r \Leftrightarrow -x \notin \alpha_r \wedge -x \neq \min(\mathbb{Q}\backslash\alpha_r)$.

$\Leftrightarrow -x \geq r \wedge -x \neq r$

$\Leftrightarrow -x > r$

$\Leftrightarrow x < -r$

$\Leftrightarrow x \in \alpha_{-r}$.

Q.E.D

Binary Operation On $\mathbb{R}$

We will now proceed to define addition and multiplication on $\mathbb{R}$. The main aim is to show that under these two binary operations, we still obtain a field.

Theorem: Addition on $\mathbb{R}$

$\exists$ a well-defined binary operation $\oplus$ on $\mathbb{R}$ given by

$\alpha \oplus \beta = \{r + s \mid r \in \alpha, s \in \beta\}$ $\forall \alpha, \beta \in \mathbb{R}$

We first show that $\oplus$ is closed.

Since $\alpha, \beta \neq \varnothing$, we obviously have $\alpha \oplus \beta \neq \varnothing$. Also, for $\varepsilon = ½$, $\exists$ $r' \in \alpha$, $s' \in \beta$ s.t $r' + ½ \notin \alpha$ and $s' + ½ \notin \beta$. Then for any $r \in \alpha$, $s \in \beta$, we have, by $\mathbb{R}$(ii), $r + s < (r' + ½) + (s' + ½) = r' + s' + 1$. In particular, we will have $r' + s' + 1 < r' + s' + 1$ if $r' + s' + 1 \in \alpha \oplus \beta$, a contradiction! Hence $\alpha \oplus \beta \neq \mathbb{Q}$, and so $\mathbb{R}$(i) holds.

For any $r \in \alpha$, $s \in \beta$, suppose $\exists$ $x \in \mathbb{Q} \backslash (\alpha \oplus \beta)$ s.t $r + s \geq x$. Then $r \geq x - s$ and by $\mathbb{R}$(ii), we have $x - s = r'$ for some $r' \in \alpha$. Hence, $x = r' + s$, i.e $x \in \alpha \oplus \beta$, a contradiction! Hence, $\mathbb{R}$(ii) holds.

For any $r \in \alpha$, $s \in \beta$, by $\mathbb{R}$(iii), $\exists$ $r' \in \alpha$, $s' \in \beta$ s.t $r' > r$, $s' > s$, i.e. $r' + s' > r + s$ and so $\max(\alpha \oplus \beta)$ cannot exist. Hence $\mathbb{R}$(iii) holds.

Hence, $\alpha \oplus \beta$ is a cut and so $\oplus$ is closed.

If $\alpha = \alpha'$ and $\beta = \beta'$, then

$\alpha \oplus \beta = \{r + s \mid r \in \alpha, s \in \beta\} = \{r + s \mid r \in \alpha', s \in \beta'\} = \alpha' \oplus \beta'$.

Hence $\oplus$ is a well-defined binary operation on $\mathbb{R}$.

Q.E.D

Theorem: Properties of addition on $\mathbb{R}$

For $\alpha, \beta, \gamma \in \mathbb{R}$, the following holds:

$A_{\mathbb{R}}$(i) $\alpha \oplus \beta = \beta \oplus \alpha$

$$\begin{aligned}\alpha \oplus \beta &= \{r + s \mid r \in \alpha, s \in \beta\} \\ &= \{s + r \mid s \in \beta, r \in \alpha\} \\ &= \beta \oplus \alpha\end{aligned}$$

$A_{\mathbb{R}}$(ii) $(\alpha \oplus \beta) \oplus \gamma = \alpha \oplus (\beta \oplus \gamma)$

$$\begin{aligned}(\alpha \oplus \beta) \oplus \gamma &= \{r + s \mid r \in \alpha, s \in \beta\} \oplus \gamma \\ &= \{(r+s) + t \mid r \in \alpha, s \in \beta, t \in \gamma\} \\ &= \{r + (s+t) \mid r \in \alpha, s \in \beta, t \in \gamma\} \\ &= \alpha \oplus \{s + t \mid s \in \beta, t \in \gamma\} \\ &= \alpha \oplus (\beta \oplus \gamma)\end{aligned}$$

$A_{\mathbb{R}}$(iii) The identity element for $\oplus$ exists and is given by α_0.

If $r + s \in \alpha \oplus \alpha_0$, then since $s < 0$, we have $r + s < r$ so that $r + s \in \alpha$ also. Hence

$\alpha \oplus \alpha_0 \subseteq \alpha$.

Conversely, take $r \in \alpha$. By $\mathbb{R}$(iii), $\exists\, r' \in \alpha$ s.t $r' > r$. Then $r - r' < 0$, i.e. $r - r' \in \alpha_0$ and since $r = r' + (r - r')$, we have $r \in \alpha \oplus \alpha_0$ and so $\alpha \oplus \alpha_0 \supseteq \alpha$.

Hence, together with $A_{\mathbb{R}}$(i), we have $\alpha \oplus \alpha_0 = \alpha = \alpha_0 \oplus \alpha$

$A_{\mathbb{R}}$(iv) For $\alpha \in \mathbb{R}$, its $\oplus$-inverse exists and is given by $-\alpha$.

Suppose $\min(\mathbb{Q}\backslash\alpha)$ does not exist. If $x \in \alpha_0$, then $x < 0$. Take $\varepsilon = -x$. Then $\exists\, y \in \alpha$ s.t $y - x \notin \alpha$, i.e. $x - y \in -\alpha$. Hence, $x = y + (x - y)$ and so $x \in \alpha \oplus (-\alpha)$.

If $x + y \in \alpha \oplus (-\alpha)$, then $-y \notin \alpha$ and so by $\mathbb{R}$(ii), $-y > x$, i.e. $x + y < 0$ and hence in α_0.

Suppose $\min(\mathbb{Q}\backslash\alpha) = r$ does exist. Then $\alpha = \alpha_r$. Also $-\alpha = \alpha_{-r}$.
Hence, $x + y \in \alpha \oplus (-\alpha) \Rightarrow x < r,\ y < -r \Rightarrow x + y < 0 \Rightarrow x + y \in \alpha_0$.
For any $x \in \alpha_0$, $x < 0$. Hence $p = r + (x/2) \in \alpha_r$ and $q = -r + (x/2) \in \alpha_{-r}$ and so
$x = p + q \in \alpha \oplus (-\alpha)$.

Hence, together with $A_{\mathbb{R}}$(i), $\alpha \oplus (-\alpha) = \alpha_0 = (-\alpha) \oplus \alpha$.

Q.E.D

Hence, this makes $(\mathbb{R}, \oplus)$ a commutative group. The definition of multiplication require that we first introduce the set of positive elements, $P_{\mathbb{R}}$.

Defn: We define the subset $P_{\mathbb{R}}$ of $\mathbb{R}$ by

$P_{\mathbb{R}} = \{\alpha \in \mathbb{R} \mid 0 \in \alpha\}$

We will also have to prove in advance the following theorem so that our definition of multiplication is well-defined.

Theorem:

For every $\alpha \in \mathbb{R}$, one and only one of the following is true:

$\alpha \in P_{\mathbb{R}}$, $-\alpha \in P_{\mathbb{R}}$, $\alpha = \alpha_0$.

We first show that at least one of them must be true. If $\alpha \notin P_{\mathbb{R}}$, then $0 \notin \alpha$. If we also have $0 \neq \min(\mathbb{Q}\backslash\alpha)$, then $0 = -0 \in -\alpha$. Otherwise, $0 = \min(\mathbb{Q}\backslash\alpha)$ and hence $\alpha = \alpha_0$.

Let $\alpha \in P_{\mathbb{R}}$. Obviously, $0 \notin \alpha_0$. So $\alpha \neq \alpha_0$. If $0 \in -\alpha$, then we require $-0 = 0 \notin \alpha$, a contradiction! Hence $-\alpha \notin P_{\mathbb{R}}$ also. If $-\alpha \in P_{\mathbb{R}}$, then we have $\alpha = -(-\alpha) \notin P_{\mathbb{R}}$ and $-\alpha \neq \alpha_0$, i.e. $\alpha \neq \alpha_0$. Finally, if $\alpha = \alpha_0$, then since $\alpha = \alpha_0 = -\alpha$, we have $\alpha \in P_{\mathbb{R}} \Leftrightarrow -\alpha \in P_{\mathbb{R}}$ which hence contradict the preceding result if either $\alpha \in P_{\mathbb{R}}$ or $-\alpha \in P_{\mathbb{R}}$ is true.

Hence, one and only one of the statements holds.

Q.E.D

We are now ready to give our definition of multiplication which is essentially a definition by cases.

Theorem: Multiplication on $\mathbb{R}$

$\exists$ a well-defined binary operation $\odot$ on $\mathbb{R}$ defined by

For α, $\beta \in P_{\mathbb{R}}$,

$\alpha \odot \beta = \{r\in\mathbb{Q} \mid r \le 0\} \cup \{r = st \mid s\in\alpha, t\in\beta, s > 0, t > 0\}$ ***M(a)***

In other cases, let

$\alpha \odot \beta = \alpha_0$ ***if*** $\alpha = \alpha_0$ ***or*** $\beta = \beta_0$ ***M(b)***

$(-\alpha) \odot (-\beta)$ ***if*** $\alpha, \beta \notin P_{\mathbb{R}} \cup \{\alpha_0\}$ ***M(c)***

$-((-\alpha) \odot \beta)$ ***if*** $\alpha \notin P_{\mathbb{R}} \cup \{\alpha_0\}, \beta\in P_{\mathbb{R}}$ ***M(d)***

$-(\alpha \odot (-\beta))$ ***if*** $\alpha\in P_{\mathbb{R}}, \beta \notin P_{\mathbb{R}} \cup \{\alpha_0\}$ ***M(e)***

We first consider only elements restricted to $P_{\mathbb{R}}$. For any $\alpha, \beta\in P_{\mathbb{R}}$, we obviously have $0\in \{r\in\mathbb{Q} \mid r \le 0\} \subseteq \alpha \odot \beta$ so $\alpha \odot \beta \ne \emptyset$. By $\mathbb{R}$(iii) and since $0\in\alpha, \beta$, $\exists\ s_1\in\alpha$, $t_1\in\beta$ s.t $s_1, t_1 > 0$. Also, $\exists\ s_2\in\alpha$, $t_2\in\beta$ s.t $s_2 +1\notin\alpha$, $t_2 +1\notin\beta$. Let $s= \max(s_1,s_2)$, $t= \max(t_1,t_2)$ and so $s\in\alpha$, $t\in\beta$, $s, t >0$ but $s+1\notin\alpha$, $t+1\notin\beta$. We claim $st+s+t+1\notin\alpha \odot \beta$. Obviously, $st+s+t+1\notin \{r\in\mathbb{Q} \mid r \le 0\}$. Hence, if $st+s+t+1\in\alpha \odot \beta$, $\exists\ s'\in\alpha$, $t'\in\beta$, $s',t' >0$ s.t $s't' =st+s+t+1$. But $\mathbb{R}$(ii) demands that $s' <s +1$, $t'< t+1$, i.e. $s't' < st+s+t+1$, a contradiction! Hence, $\mathbb{R}$(i) holds.

Take any $r\in\alpha \odot \beta$ and $s\notin\alpha \odot \beta$ and suppose $r\ge s$. Obviously, $r\ne s$ and since $s\notin\alpha\odot \beta \Rightarrow s>0$, we have $r > s >0$. Let $t= r/s >1$ and so $st = r$. Now, since $r \in\alpha \odot \beta$ and $r\notin \{r\in\mathbb{Q} \mid r \le 0\}$, $\exists\ s'\in\alpha$, $t'\in\beta$, $s' ,t' >0$ s.t $r = s't'$. Hence $st =s't'$, and so $s=(s't')/t$. But $s'/t< s'$, i.e. $s'/t \in\alpha$. Since $t'\in\beta$ also and $s'/t, t'>0$, we are forced to conclude that $s\in\alpha \odot \beta$, a contradiction! Hence, $\mathbb{R}$(ii) holds.

Take any $r\in\alpha \odot \beta$. We may assume $r= st$ for some $s\in\alpha$, $t\in\beta$, $s,t >0$ for otherwise, $r\le 0$ and we can just take any $s'\in\alpha$, $t'\in\beta$, $s' ,t' >0$ and we will have $s't'> 0\ge r$. By $\mathbb{R}$(iii), $\exists\ s'\in\alpha$ s.t $s' >s >0$, $t'\in\beta$ s.t $t' >t >0$ and so $s't'> st = r$. Hence, $\mathbb{R}$(iii) holds.

Hence, $\alpha \odot \beta$ is also a cut for $\alpha, \beta\in P_{\mathbb{R}}$.

Now let $\alpha =\alpha'$, $\beta =\beta'$ where $\alpha, \beta\in P_{\mathbb{R}}$.

$$\begin{aligned}\alpha \odot \beta &= \{r\in\mathbb{Q} \mid r \le 0\} \cup \{r = st \mid s\in\alpha, t\in\beta, s > 0, t > 0\}\\ &= \{r\in\mathbb{Q} \mid r \le 0\} \cup \{r = st \mid s\in\alpha', t\in\beta', s > 0, t > 0\}\\ &= \alpha' \odot \beta'\end{aligned}$$

Hence, $\odot$ is well defined for elements restricted to $P_{\mathbb{R}}$.

Observe that for all other cases, $\alpha \odot \beta$ is defined in terms of α_0, operation of $\odot$ on elements in $P_{\mathbb{R}}$ or by taking the negative. Hence, $\alpha \odot \beta$ remains a cut since these are cut-preserving operations. Since we have shown $\odot$ is a function on $P_{\mathbb{R}}$X $P_{\mathbb{R}}$ and as the negative is unique, $\odot$ will be a function when restricted to each sub cases. As the sub cases are all disjoint and covers $\mathbb{R}$, $\odot$ will be a function on $\mathbb{R}$X$\mathbb{R}$.

Hence, $\odot$ is well defined on $\mathbb{R}$.

Q.E.D

The proofs for the properties of multiplication also requires us to consider various cases but the job is made easy by the following lemma, which actually follows directly from definition. We are simply just doing some algebraic verification in the lemma, tedious but easy.

Lemma:

For any $\alpha, \beta \in \mathbb{R}$, we have

$-(\alpha \odot \beta) = (-\alpha) \odot \beta = \alpha \odot (-\beta)$

M(a):

$-(\alpha \odot \beta) = -(\alpha \odot (-(-\beta)))$

$= \alpha \odot (-\beta)$ (defn M(e))

$-(\alpha \odot \beta) = -((-(-\alpha)) \odot \beta)$

$= -(\alpha) \odot \beta$ (defn M(d))

M(b):

$-(\alpha \odot \beta) = -(\alpha_0) = \alpha_0 = (-\alpha) \odot \beta$

$-(\alpha \odot \beta) = -(\alpha_0) = \alpha_0 = \alpha \odot (-\beta)$

M(c):

$-(\alpha \odot \beta) = -((-\alpha) \odot (-\beta))$

$= (-\alpha) \odot \beta$ (defn M(e))

$-(\alpha \odot \beta) = -((-\alpha) \odot (-\beta))$

$= \alpha \odot (-\beta)$ (defn M(d))

M(d):

$-(\alpha \odot \beta) = -(-((-\alpha) \odot \beta))$

$= (-\alpha) \odot \beta$

$-(\alpha \odot \beta) = -(-((-\alpha) \odot \beta))$

$= (-\alpha) \odot \beta$

$= \alpha \odot (-\beta)$ (defn M(c))

M(e):

$-(\alpha \odot \beta) = -(-(\alpha \odot (-\beta)))$

$= \alpha \odot (-\beta)$

$-(\alpha \odot \beta) = -(-(\alpha \odot (-\beta)))$

$= \alpha \odot (-\beta)$

$= (-\alpha) \odot \beta$ (defn M(c))

Hence, $-(\alpha \odot \beta) = (-\alpha) \odot \beta = \alpha \odot (-\beta)$.

Q.E.D

We can now introduce the reciprocal cut of a positive cut, which is essentially the multiplicative inverse of that cut.

Theorem: The reciprocal cut

For any $\alpha \in P_{\mathbb{R}}$, the set defined by

$\alpha^{-1} = \{r \in \mathbb{Q} \mid r \leq 0 \} \cup \{ r = 1/s \mid s \notin \alpha, s > 0 \text{ and } s \neq \min(\mathbb{Q} \setminus \alpha) \}$

is a cut. We call this the reciprocal cut of α.

Since $0 \in \alpha^{-1}$, $\alpha^{-1} \neq \varnothing$. Furthermore, since $0 \in \alpha$, $\exists$ s >0 s.t $s \in \alpha$, by $\mathbb{R}$(iii). Also, 1/s> 0 and so $1/s \notin \alpha^{-1}$. Hence, $\alpha^{-1} \neq \mathbb{Q}$.

Hence $\mathbb{R}$(i) holds.

Let $r\in\alpha^{-1}$ and $t\notin\alpha^{-1}$. If $r \le 0$, then we trivially have $r \le 0 < t$. Otherwise, $r > 0$ and we must have $1/r\notin\alpha$, $1/r > 0$ and $1/r \neq \min(\mathbb{Q}\backslash\alpha)$. Since $t\notin\alpha^{-1}$, $t > 0$ and so $1/t > 0$. If $1/t = \min(\mathbb{Q}\backslash\alpha)$, then since $1/r\notin\alpha$ and $1/r \neq \min(\mathbb{Q}\backslash\alpha)$, we have $1/t < 1/r$, i.e. $r < t$. If $1/t \neq \min(\mathbb{Q}\backslash\alpha)$, then we must have $1/t\in\alpha$, else $t\in\alpha^{-1}$. Hence, by $\mathbb{R}$(ii), $1/t < 1/r$, i.e. $r < t$ again.

Hence $\mathbb{R}$(ii) holds.

Take any $r\in\alpha^{-1}$. $\exists\ s\notin\alpha$ by $\mathbb{R}$(i). By $\mathbb{R}$(ii), we have $s + 1 > s > 0$. Hence, if $r \le 0$, we have $1/(s+1)\in\alpha^{-1}$ and $r \le 0 < 1/(s+1)$. We consider then only $r > 0$. We must then have $1/r\notin\alpha$, $1/r > 0$ and $1/r \neq \min(\mathbb{Q}\backslash\alpha)$. Since $1/r \neq \min(\mathbb{Q}\backslash\alpha)$, $\exists\ s\notin\alpha$ s.t $1/r > s$. By density theorem, $\exists$ t s.t $1/r > t > s$. Then $t\notin\alpha$, $t > 0$ and $t \neq \min(\mathbb{Q}\backslash\alpha)$. Also, $1/t > r$ and $1/t\in\alpha^{-1}$.

Hence, $\mathbb{R}$(iii) holds.

Hence, α^{-1} is also a cut.

Q.E.D

Just like what we do for the negative cut, the following lemma tells us the exact form of the reciprocal cut of a positive rational cut.

Lemma:

For any $\alpha_r\in P_{\mathbb{R}}$, its reciprocal cut is $\alpha_{1/r}$.

Take any $x\in(\alpha_r)^{-1}$. If $x \le 0$, then $x \le 0 < 1/r$ and so $x\in\alpha_{1/r}$. Otherwise, $1/x > 0$, $1/x\notin\alpha_r$, $1/x \neq \min(\mathbb{Q}\backslash\alpha_r) = r$. Hence $1/x > r$, i.e. $x < 1/r$ and so $x\in\alpha_{1/r}$ also.

Take any $x\in\alpha_{1/r}$. If $x \le 0$, then trivially $x\in(\alpha_r)^{-1}$. Hence, consider $0 < x < 1/r$. We have $0 < r < 1/x$. Hence $1/x > 0$, $1/x\notin\alpha_r$ and $1/x \neq r = \min(\mathbb{Q}\backslash\alpha_r)$. This mean $x = 1/(1/x)\in(\alpha_r)^{-1}$.

Hence, $(\alpha_r)^{-1} = \alpha_{1/r}$.

Q.E.D

After so many detours, we can now finally properly prove the properties for multiplication. The good news is that we have not done 'extra' work. We have only actually proved some results in advance so we may expect relatively lessor work in the following few sections.

Theorem: Properties of multiplication on $\mathbb{R}$

$\forall\ \alpha, \beta, \gamma\in P_{\mathbb{R}}$, we have

m$_{\mathbb{R}}$(i) $\alpha \odot \beta = \beta \odot \alpha$

$\alpha \odot \beta = \{r\in\mathbb{Q} \mid r \le 0\} \cup \{r = st \mid s\in\alpha, t\in\beta, s > 0, t > 0\}$

$= \{r\in\mathbb{Q} \mid r \le 0\} \cup \{r = ts \mid t\in\beta, s\in\alpha, t > 0, s > 0\}$

$= \beta \odot \alpha$

m$_{\mathbb{R}}$(ii) $(\alpha \odot \beta) \odot \gamma = \alpha \odot (\beta \odot \gamma)$

$(\alpha \odot \beta) \odot \gamma = \{r\in\mathbb{Q} \mid r \le 0\} \cup \{r = uv \mid u\in\alpha \odot \beta, v\in\gamma, u > 0, v > 0\}$

$\alpha \odot (\beta \odot \gamma) = \{r\in\mathbb{Q} \mid r \le 0\} \cup \{r = uv \mid u\in\alpha, v\in\beta \odot \gamma, u > 0, v > 0\}$

We need only to show

$\{r = uv \mid u\in \alpha \odot \beta, v\in\gamma, u, v > 0\} = \{r = uv \mid u\in \alpha, v\in \beta \odot \gamma, u > 0, v > 0\}$

Take $uv\in \{r = uv \mid u\in \alpha \odot \beta, v\in\gamma, u, v > 0\}$. Since $u > 0$, $\exists\, s', t' > 0$ s.t $s'\in \alpha$, $t'\in \beta$ and $s't' = u$. Note that $t'v > 0$. Hence

$uv = (s't')v = s'(t'v)\in \{r = uv \mid u\in \alpha, v\in \beta \odot \gamma, u > 0, v > 0\}$.

Take $uv\in \{r = uv \mid u\in \alpha, v\in \beta \odot \gamma, u > 0, v > 0\}$. Since $v > 0$, $\exists\, s', t' > 0$ s.t $s'\in \beta$, $t'\in\gamma$ and $s't' = v$. Note that $us' > 0$. Hence

$uv = u(s't') = (us')t'\in \{r = uv \mid u\in \alpha \odot \beta, v\in\gamma, u, v > 0\}$.

Hence, $(\alpha \odot \beta) \odot \gamma = \alpha \odot (\beta \odot \gamma)$

m$_{\mathbb{R}}$(iii) The identity element exist and is given by α_1.

First, note that $0 < 1$ and so $0\in \alpha_1$, i.e. $\alpha_1\in P_{\mathbb{R}}$. Now,

$\alpha \odot \alpha_1 = \{r\in \mathbb{Q} \mid r \le 0\} \cup \{r = st \mid s\in \alpha, t\in \alpha_1, s > 0, t > 0\}$

$\qquad\quad = \{r\in \mathbb{Q} \mid r \le 0\} \cup \{r = st \mid s\in \alpha, s > 0, 1 > t > 0\}$

Take $r\in \alpha \odot \alpha_1$. If $r \le 0$, then since $0\in \alpha$, obviously, $r\in \alpha$ by $\mathbb{R}$(ii). Otherwise, $\exists\, s\in \alpha$, $0 < t < 1$ s.t $st = r$. Hence $r = st < s$ and by $\mathbb{R}$(ii), $r\in \alpha$ also. Now take $s\in \alpha$. If $s \le 0$, we have $s\in \{r\in \mathbb{Q} \mid r \le 0\}$ and hence in $\alpha \odot \alpha_1$. Otherwise, by $\mathbb{R}$(iii), $\exists\, s'\in \alpha$ s.t $s' > s > 0$. Hence, let $t = s/s'$ and we have $0 < t < 1$ and so $s = s't \in \alpha \odot \alpha_1$. Hence, together with m$_{\mathbb{R}}$(i),

$\alpha \odot \alpha_1 = \alpha = \alpha_1 \odot \alpha$.

m$_{\mathbb{R}}$(iv) For each $\alpha\in P_{\mathbb{R}}$, its $\odot$-inverse exists and is given by α^{-1}.

$\alpha \odot \alpha^{-1} = \{r\in \mathbb{Q} \mid r \le 0\} \cup \{r = st \mid s\in \alpha, t\in \alpha^{-1}, s > 0, t > 0\}$

Take $r\in \alpha \odot \alpha^{-1}$. If $r \le 0$, then obviously $r\in \alpha_1$. Otherwise, $\exists\, s\in \alpha$, $t\in \alpha^{-1}$, $s, t > 0$ s.t $r = st$. As $t > 0$, we must have $1/t\notin \alpha$, $1/t > 0$ and $1/t \ne \min(\mathbb{Q}\backslash\alpha)$. In particular, by $\mathbb{R}$(ii), $1/t > s$, i.e. $1 > st = r$ and so $r\in \alpha_1$. Now take any $r\in \alpha_1$, i.e. $r < 1$. Since $r \le 0$ means immediately that $r\in \alpha \odot \alpha^{-1}$, we need only consider $0 < r < 1$. Since $0\in \alpha$, $\exists\, s_1\in \alpha$, $s_1 > 0$ by $\mathbb{R}$(iii). Also, for $\varepsilon = (s_1(1 - r))/r > 0$, $\exists\, s_2\in \alpha$ s.t $s_2 + \varepsilon\notin \alpha$. We may assume $s_2 + \varepsilon \ne \min(\mathbb{Q}\backslash\alpha)$ for otherwise, by $\mathbb{R}$(iii), $\exists\, s_3\in \alpha$ s.t $s_3 > s_2$ and hence $s_3 + \varepsilon > s_2 + \varepsilon$, i.e. $s_3 + \varepsilon \ne\min(\mathbb{Q}\backslash\alpha)$ and we can just take s_2 to be s_3. Hence, let $s = \max(s_1, s_2)$. Then $s + \varepsilon > 0$, $s + \varepsilon\notin \alpha$ and $s + \varepsilon \ne \min(\mathbb{Q}\backslash\alpha)$. Hence $1/(s + \varepsilon)\in \alpha^{-1}$. Hence, $s/(s + \varepsilon)\in \alpha \odot \alpha^{-1}$. But

$s/(s + \varepsilon) = s/(s + (s_1(1 - r))/r)$

$\qquad\qquad \ge s/(s + (s(1 - r))/r)$ ($\because s \ge s_1$)

$\qquad\qquad =r$

By $\mathbb{R}$(ii), this means $r\in \alpha \odot \alpha^{-1}$. Hence, together with m$_{\mathbb{R}}$(i), we have

$\alpha \odot \alpha^{-1} = \alpha_1 = \alpha^{-1} \odot \alpha$.

m$_{\mathbb{R}}$(v) $\alpha \odot (\beta \oplus \gamma) = (\alpha \odot \beta) \oplus (\alpha \odot \gamma)$

$\alpha \odot (\beta \oplus \gamma) = \{ r\in \mathbb{Q} \mid r \le 0\} \cup \{r = st \mid s\in \alpha, t\in \beta \oplus \gamma, s > 0, t > 0\}$

$(\alpha \odot \beta) \oplus (\alpha \odot \gamma) = \{s + t \mid s\in \alpha \odot \beta, t\in \alpha \odot \gamma\}$

Take any $r \in \alpha \odot (\beta \oplus \gamma)$. If $r \leq 0$, then $r \in \alpha \odot \beta$. Also, $0 \in \alpha \odot \gamma$ so $r = r + 0 \in (\alpha \odot \beta) \oplus (\alpha \odot \gamma)$. Hence, consider $r > 0$. Then $r = s(t + k)$ where $s \in \alpha$, $t \in \beta$, $k \in \gamma$, and $s, t + k > 0$. Since $t + k > 0$, we have the following cases:

(i) $t \leq 0, k > 0$

Hence, $st \leq 0$, i.e. $st \in \alpha \odot \beta$. Also, $s \in \alpha$, $k \in \gamma$ and $s, k > 0 \Rightarrow sk \in \alpha \odot \gamma$. Hence, $r = st + sk \in (\alpha \odot \beta) \oplus (\alpha \odot \gamma)$.

(ii) $t > 0, k \leq 0$

Hence, $sk \leq 0$, i.e. $sk \in \alpha \odot \gamma$. Also, $s \in \alpha$, $t \in \beta$ and $s, t > 0 \Rightarrow st \in \alpha \odot \beta$. Hence, $r = st + sk \in (\alpha \odot \beta) \oplus (\alpha \odot \gamma)$.

(iii) $t > 0, k > 0$

Then $s \in \alpha$, $t \in \beta$, $s, t > 0 \Rightarrow st \in (\alpha \odot \beta)$. Similarly, $s \in \alpha$, $k \in \gamma$, $s, k > 0 \Rightarrow sk \in \alpha \odot \gamma$. Hence, $r = st + sk \in (\alpha \odot \beta) \oplus (\alpha \odot \gamma)$.

Hence $r \in (\alpha \odot \beta) \oplus (\alpha \odot \gamma)$.

Now take any $r \in (\alpha \odot \beta) \oplus (\alpha \odot \gamma)$. If $r \leq 0$, then clearly $r \in \alpha \odot (\beta \oplus \gamma)$. Hence, consider $r > 0$. Then $\exists\ s \in (\alpha \odot \beta)$, $t \in (\alpha \odot \gamma)$ s.t $r = s + t$. Since $s + t > 0$, we have the following cases:

(i) $s > 0, t > 0$

Then $\exists\ p, p' \in \alpha$, $q \in \beta$, $u \in \gamma$, $p, p', q, u > 0$ s.t $s = pq$ and $t = p'u$. If $p = p'$, then $r = p(q + u) \in \alpha \odot (\beta \oplus \gamma)$. Hence, consider $p' < p$, i.e. $p'/p < 1$. Then $r = pq + p'u = p(q + (p'/p)u)$. But $(p'/p)u < u \in \gamma$, and so $(p'/p)u \in \gamma$. Hence $r \in \alpha \odot (\beta \oplus \gamma)$. Similarly, if $p < p'$, we consider $r = p'((p/p')q + u)$ and so $r \in \alpha \odot (\beta \oplus \gamma)$ also.

(ii) $s \leq 0, t > 0$

$\exists\ p \in \alpha$, $q \in \gamma$, $p, q > 0$ s.t $t = pq = p(0 + q) \in \alpha \odot (\beta \oplus \gamma)$. Then $r = s + t \leq t$ and so $r \in \alpha \odot (\beta \oplus \gamma)$ also.

(iii) $s > 0, t \leq 0$

Similarly, $\exists\ p \in \alpha$, $q \in \beta$ s.t $s = pq = p(q + 0) \in \alpha \odot (\beta \oplus \gamma)$. Then $r = s + t \leq s$ and so $r \in \alpha \odot (\beta \oplus \gamma)$ also.

Hence, $r \in \alpha \odot (\beta \oplus \gamma)$.

Hence,

$\alpha \odot (\beta \oplus \gamma) = (\alpha \odot \beta) \oplus (\alpha \odot \gamma)$.

Now that we have shown $m_{\mathbb{R}}$(i) to $m_{\mathbb{R}}$(v), it is easy to see that they actually hold for the whole of $\mathbb{R}$. With the relation $-(\alpha \odot \beta) = (-\alpha) \odot \beta = \alpha \odot (-\beta)$, we can 'extract' out all the negative signs until the elements we are considering are all in $P_{\mathbb{R}}$. We can then invoke the relevant $m_{\mathbb{R}}$, achieve the required form and then "return" the negative signs back to the elements again.

For example, for $\alpha, \beta \in P_{\mathbb{R}}$, $\gamma \notin P_{\mathbb{R}} \cup \{\alpha_0\}$, we will have

$$\begin{aligned}(\alpha \odot \beta) \odot \gamma &= (\alpha \odot \beta) \odot (-(-\gamma)) \\ &= -((\alpha \odot \beta) \odot (-\gamma))\end{aligned}$$

$= -(\alpha \odot (\beta \odot (-\gamma)))$ (by $m_{\mathbb{R}}$(ii))
$= \alpha \odot (-(\beta \odot (-\gamma)))$
$= \alpha \odot (\beta \odot (-(-\gamma)))$
$= \alpha \odot (\beta \odot \gamma)$

We will not explicitly repeat the above for all the various cases since they are essentially direct consequences of the $m_{\mathbb{R}}$'s and the result $-(\alpha\odot\beta)=(-\alpha)\odot\beta=\alpha\odot(-\beta)$. In fact, this 'nice' situation is 'built into' our definition of $\odot$ as $\odot$ is basically defined with reference to elements in $P_{\mathbb{R}}$. Take note, though, that for $\alpha \notin P_{\mathbb{R}} \cup \{\alpha_0\}$, its inverse is given by $\alpha^{-1}=-(-\alpha)^{-1}$. Hence, we conclude that $M_{\mathbb{R}}$(i) to $M_{\mathbb{R}}$(v) is also true, where the results are extended to the whole of $\mathbb{R}$.

Q.E.D

Hence, we have managed to show that $(\mathbb{R},\oplus, \odot)$ is a field. The next natural thing to do is to order our field.

<u>Order On $\mathbb{R}$</u>

We have already defined our set of positive elements, $P_{\mathbb{R}}$, and have in fact shown one of the two criteria required for it to be the set of positive elements. The following theorem sums up everything.

<u>Theorem:</u>

The subset $P_{\mathbb{R}}$ is closed under $\oplus$ and $\odot$. Furthermore, for every $\alpha\in\mathbb{R}$, exactly one of the following is true: $\alpha = \alpha_0$, $\alpha\in P_{\mathbb{R}}$, $-\alpha\in P_{\mathbb{R}}$.

Take any $\alpha, \beta \in P_{\mathbb{R}}$.

Since $0\in\alpha, \beta$, we will have $0 = 0 + 0\in\alpha \oplus \beta$ and so $\alpha \oplus \beta\in P_{\mathbb{R}}$. Also, $0\in \{r\in\mathbb{Q} \mid r \leq 0\} \subseteq \alpha \odot \beta$ and so $\alpha \odot \beta\in P_{\mathbb{R}}$. Hence $P_{\mathbb{R}}$ is closed under $\oplus$ and $\odot$. We have already proven the second claim.

Q.E.D

The natural definition for order now follows.

Defn: For any $\alpha, \beta\in\mathbb{R}$, we say α is greater than β and write $\alpha \succ \beta$ if $\alpha \oplus (-\beta)\in P_{\mathbb{R}}$. We write $\alpha \succcurlyeq \beta$ if $\alpha \succ \beta$ or $\alpha = \beta$.

This definition makes $(\mathbb{R}, \oplus, \odot, \succ)$ an ordered field. The next theorem unravel the microscopic meaning of this abstract order in terms of set relation between cuts.

<u>Theorem:</u>

$\alpha \succ \beta$ iff $\alpha \supset \beta$.

Suppose $\alpha \succ \beta$. Then $\alpha \oplus (-\beta)\in P_{\mathbb{R}}$. Take any $r\in\beta$. Then we cannot have $-r\in-\beta$. Since $0\in\alpha \oplus (-\beta)$, $\exists$ $s\in\alpha$, $t\in-\beta$ s.t $s + t = 0$, i.e. $s = -t$. By $\mathbb{R}$(ii), $-r > t$, i.e. $r < -t = s$

and so by $\mathbb{R}$(ii) again, $r\in\alpha$. Hence $\alpha \supseteq \beta$. If $\alpha = \beta$, then we have $\alpha \oplus (-\beta) = \alpha \oplus (-\alpha) = \alpha_0(\notin P_{\mathbb{R}})$, a contradiction! Hence $\alpha \supset \beta$.

Now suppose $\alpha \supset \beta$. This means $\exists$ $r\in\alpha$ but $r\notin\beta$. By $\mathbb{R}$(iii), $\exists$ $r'\in\alpha$ s.t $r' > r$. By $\mathbb{R}$(ii), $r'\notin\beta$ also. Hence, $r'\notin\beta$, $r' \neq \min(\mathbb{Q}\backslash\beta)$ and so $-r'\in-\beta$. This means $0 = r' + (-r')\in\alpha \oplus (-\beta)$ so $\alpha \oplus (-\beta)\in P_{\mathbb{R}}$, i.e. $\alpha \succ \beta$.

Hence, $\alpha \succ \beta$ iff $\alpha \supset \beta$.

Trivially, we also have $\alpha \succcurlyeq \beta$ iff $\alpha \supseteq \beta$.

Q.E.D

The Dedekind Real Number System

Any real number system that one can conceive of must certainly contain a copy of the rationals. We shall now show that our system of Dedekind's cuts indeed contain the Field of rationals.

Lemma:

For any rational cuts α_x, α_y, we have

(a) $\alpha_x \oplus \alpha_y = \alpha_{x+y}$

(b) $\alpha_x \odot \alpha_y = \alpha_{xy}$

(a) Take any $r + s\in\alpha_x \oplus \alpha_y$. Then $r < x$, $s < y$ so that $r + s < x + y$, i.e. $r + s\in\alpha_{x+y}$. Now take $z\in\alpha_{x+y}$. Then $z < x + y$, i.e. $z - x < y$. By the density theorem for $\mathbb{Q}$, $\exists$ z' s.t $z - x < z' < y$. Then $z'\in\alpha_y$ and let $\varepsilon = z' - (z - x) > 0$. Now, $x - \varepsilon < x$ so that $x - \varepsilon\in\alpha_x$. Hence, $z = z' + (x - \varepsilon)\in\alpha_x \oplus \alpha_y$.

Hence, $\alpha_x \oplus \alpha_y = \alpha_{x+y}$.

(b) We consider first $\alpha_x, \alpha_y\in P_{\mathbb{R}}$. Take $r\in\alpha_x \odot \alpha_y$. If $r \leq 0$, then since $x, y > 0$, we have $xy > 0 \geq r$ so that $r\in\alpha_{xy}$. Hence, we consider $r>0$ so that $r = st$ where $0 < s<x$, $0 < t < y$. This means $r = st < xy$ and so $r\in\alpha_{xy}$ also. Now take $r\in\alpha_{xy}$. If $r \leq 0$, we trivially have $r\in\alpha_x\odot\alpha_y$. Hence consider $0 < r < xy$. Then $0 < (xy - r)/y$. By density theorem, $\exists$ $0 < \varepsilon_1 < (xy - r)/y$. Similarly, $\exists$ $0 < \varepsilon_2 < x$. Take $\varepsilon = \min(\varepsilon_1, \varepsilon_2)$.

$$\begin{aligned} r/(x - \varepsilon) &< r/(x - ((xy - r)/y)) \\ &= y \end{aligned}$$

Obviously, $0<x - \varepsilon < x$. Hence, $r = (x - \varepsilon)(r/(x - \varepsilon))\in\alpha_x\odot\alpha_y$. Hence, $\alpha_x\odot\alpha_y=\alpha_{xy}$. To see that the result holds true for all rational cuts, we can either employ the fact that $-(\alpha \odot \beta) = (-\alpha) \odot \beta = \alpha \odot (-\beta)$ as mentioned earlier or even by simply noting that $-\alpha_r = \alpha_{-r}$.

Q.E.D.

Theorem:

$(\mathbb{R}_{\mathbb{Q}}, \oplus, \odot, \succ)$ is a subfield of $(\mathbb{R}, \oplus, \odot, \succ)$. Furthermore, $(\mathbb{R}_{\mathbb{Q}}, \oplus, \odot, \succ)$ is isomorphic to $(\mathbb{Q}, +, ., >)$.

Take any $\alpha_x, \alpha_y\in \mathbb{R}_{\mathbb{Q}}$,

$$\begin{aligned} \alpha_x \oplus (-\alpha_y) &= \alpha_x \oplus \alpha_{-y} \\ &= \alpha_{x-y} \quad (\in \mathbb{R}_{\mathbb{Q}}) \end{aligned}$$

$\alpha_x \odot (\alpha_y)^{-1} = \alpha_x \odot \alpha_{1/y}$ ($\forall\ \alpha_y \neq \alpha_0$)

$= \alpha_{x/y}$ ($\in \mathbb{R}_{\mathbb{Q}}$)

Obviously, $\alpha_1 \in \mathbb{R}_{\mathbb{Q}}$. Hence, $(\mathbb{R}_{\mathbb{Q}}, \oplus, \odot, \succ)$ is a subfield of $(\mathbb{R}, \oplus, \odot, \succ)$.

Consider the mapping ϕ: $\mathbb{R}_{\mathbb{Q}} \to \mathbb{Q}$ given by

$\phi(\alpha_r) = r\ \ \forall\ \alpha_r \in \mathbb{R}_{\mathbb{Q}}$.

We have shown that $\alpha_r = \alpha_s \Rightarrow r = s$. Hence, ϕ is a well-defined function.

We have also shown that $r = s \Rightarrow \alpha_r = \alpha_s$, so ϕ is one-one.

For any $r \in \mathbb{Q}$, take $\alpha_r \in \mathbb{R}_{\mathbb{Q}}$ so that $\phi(\alpha_r) = r$. Hence, ϕ is onto.

Hence, ϕ is a bijective function.

Take any $\alpha_r, \alpha_s \in \mathbb{R}_{\mathbb{Q}}$.

$$\begin{aligned}\phi(\alpha_r \oplus \alpha_s) &= \phi(\alpha_{r+s})\\ &= r + s\\ &= \phi(\alpha_r) + \phi(\alpha_s)\end{aligned}$$

$$\begin{aligned}\phi(\alpha_r \odot \alpha_s) &= \phi(\alpha_{r\,.\,s})\\ &= r\,.\,s\\ &= \phi(\alpha_r)\,.\,\phi(\alpha_s)\end{aligned}$$

$$\begin{aligned}\alpha_r \succ \alpha_s &\Rightarrow \alpha_r \oplus \alpha_{-s} \in P_{\mathbb{R}}\\ &\Rightarrow \alpha_{r-s} \in P_{\mathbb{R}}\\ &\Rightarrow 0 \in \alpha_{r-s}\\ &\Rightarrow 0 < r - s\\ &\Rightarrow s < r\\ &\Rightarrow \phi(\alpha_r) > \phi(\alpha_s)\end{aligned}$$

Hence, $(\mathbb{R}_{\mathbb{Q}}, \oplus, \odot, \succ) \simeq (\mathbb{Q}, +, ., >)$.

Q.E.D

The next theorem finally tells us that Dedekind has managed to extend the Field of rational to an order complete field.

Theorem:

$(\mathbb{R}, \oplus, \odot, \succ)$ is order complete.

Take any non-empty subset A of $\mathbb{R}$ that is bounded above by some $\beta \in \mathbb{R}$, i.e. $\alpha \preccurlyeq \beta$ $\forall\ \alpha \in A$. Define

$\gamma = \{r \in \mathbb{Q} \mid r \in \alpha \text{ for some } \alpha \in A\}$.

We first show that $\gamma \in \mathbb{R}$.

Since $A \neq \varnothing$, $\exists\ \alpha_0 \in A$. By $\mathbb{R}$(i), $\alpha_0 \neq \varnothing$. Since $\alpha_0 \subseteq \gamma$, $\gamma \neq \varnothing$ also. Now, by $\mathbb{R}$(i), $\beta \neq \mathbb{Q}$. We have $\alpha \preccurlyeq \beta$, i.e. $\alpha \subseteq \beta$ $\forall\ \alpha \in A$. Hence, we must also have $\gamma \subseteq \beta$, i.e. $\gamma \neq \mathbb{Q}$. Hence $\mathbb{R}$(i) holds.

Let $r \in \gamma$ and $s \notin \gamma$. Then $r \in \alpha$ for some $\alpha \in A$. Since $s \notin \gamma$, $s \notin \alpha$ also. By $\mathbb{R}$(ii), we then have $r < s$. Hence $\mathbb{R}$(ii) holds.

Suppose $\max(\gamma)$ exists. Then $\max(\gamma) \in \alpha$ for some $\alpha \in A$. In particular, since $r \in \alpha \Rightarrow r \in \gamma \Rightarrow r \leq \max(\gamma)$, we have $\max(\gamma) = \max(\alpha)$, contradicting $\mathbb{R}$(iii)! Hence, $\mathbb{R}$(iii) holds.

Hence $\gamma \in \mathbb{R}$.

Clearly, $\alpha \subseteq \gamma$, i.e. $\alpha \preccurlyeq \gamma \; \forall \; \alpha \in A$. Hence, γ is an upper bound of A. Also, we have shown that $\gamma \subseteq \beta$, i.e. $\gamma \preccurlyeq \beta$. Since β is any arbitrarily upper bound of A, we conclude $\gamma = \text{SupA}$.

Hence, $(\mathbb{R}, \oplus, \odot, \succ)$ has the least upper bound property, i.e. it is order complete.

Q.E.D

Dedekind's cut is in fact a particular realization of a Dedekind real number system, which is being given its formal definition below.

Defn: An ordered field ($\mathbb{R}_D$, $\oplus$,$\odot$, $\succ$) is called a Dedekind real number system if

(i) There exist a subfield ($\mathbb{Q}_D$, $\oplus$,$\odot$, $\succ$) which is isomorphic to ($\mathbb{Q}$,+,.,>).

(ii) ($\mathbb{R}_D$, $\oplus$,$\odot$, $\succ$) is order complete.

This definition may be a bit disheartening, since this means that what we have achieved so far is only to show the existence of a Dedekind real number system. But there are more to explore in this definition and we shall attempt to do so in the next section. Since we really have no need to use the particular structure of the system of Dedekind's cuts, we shall henceforth speak only of a general Dedekind real number system denoted by ($\mathbb{R}$, +,. ,>). The various important subsets of natural numbers, integers and rationals will be naturally denoted by $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ respectively. Note that we are now still on rather shaky ground since we do not know whether Dedekind real number systems are unique. If it is not, then it is definitely a bad model of the real numbers. This chapter will culminate with the proof that Dedekind real number systems are indeed unique, lending support that the Dedekind real number system is a good model for the real numbers.

Properties Of Dedekind Real Number Systems

Most of the results proven here are usually regarded as properties fundamental to the real numbers. Order completeness of Dedekind real number systems are invoked in most of the proofs, and this may be how Dedekind stumble upon the idea that order completeness may just be the 'essence' of the real numbers. We will start off with the Archimedean Property, which incidentally also employ the fact that Dedekind real number systems are order complete.

Theorem: Archimedean Property

Let $x, y \in \mathbb{R}$, $x>0$. Then $\exists \, n \in \mathbb{N}$ s.t $nx > y$.

Let $A=\{nx | \, n \in \mathbb{N}\}$. Suppose that the claim do not hold, then A is bounded above by y. By order completeness, SupA exists. Since x>0, SupA-x<SupA and hence SupA-x is not an upper bound for A. Hence, $\exists$ m$\in \mathbb{N}$ s.t SupA-x<mx, i.e SupA<(m+1)x. But (m+1)x $\in$A and this contradict the fact that SupA is an upper bound for A! Since the falsity of the claim leads to a contradiction, the claim must be true.

Q.E.D

The following lemma shows some simple consequences of the Archimedean Property in $\mathbb{R}$. We prove them here so that the various forms can be invoked directly in subsequent proofs.

Lemma:

Let x, y∈ $\mathbb{R}$. Then the following holds:

(i) ***∃ n∈ $\mathbb{N}$ s.t n>y.***

(ii) ***if x>0, then ∃ n∈ $\mathbb{N}$ s.t x>1/n***

(iii) ***if y≥0, then ∃ n∈ $\mathbb{N}$ s.t n-1≤y<n.***

(i) This is a special case of Archimedean Property for x=1>0

(ii) By Archimedean Property, for y=1, ∃ n∈ $\mathbb{N}$ s.t nx>1,i.e x>1/n.

(iii) Consider the set A={m∈ $\mathbb{N}$ | y<m}. (i) ensures that A is not empty. Hence, since $\mathbb{N}$ is well-ordered, MinA =n exist. Then n-1∉ A. We consider 2 cases:

a) n-1 ∈ $\mathbb{N}$
Then we must have n-1≤y<n by the defining property of A.

b) n-1 ∉ $\mathbb{N}$
Then n-1=0. Hence, n-1=0≤y<n.

Q.E.D

Before we prove the density theorem, we need to show the existence of at least one non-rational point. This follows quite easily from Order completeness in $\mathbb{R}$ and the fact that $\mathbb{Q}$ is not order complete as shown in the following lemma.

Lemma:

$\mathbb{R}$\ $\mathbb{Q}$ is not empty.

Suppose not. Since $\mathbb{Q}$⊆$\mathbb{R}$, we have $\mathbb{Q}$=$\mathbb{R}$. Hence, ($\mathbb{Q}$, +,. ,>) = ($\mathbb{R}$, +,. ,>) which is order complete. But ($\mathbb{Q}$, +,. ,>) is not order complete! Hence, $\mathbb{R}$\$\mathbb{Q}$ cannot be empty.

We call elements in $\mathbb{R}$\$\mathbb{Q}$ **irrational points**.

Q.E.D

We can now prove the density theorem, which tells us that both the rational and irrational points are dense on the number line.

Theorem: Density theorem

Let x, y∈ $\mathbb{R}$ be s.t x<y. Then ∃ r∈ $\mathbb{Q}$, z∈ $\mathbb{R}$\ $\mathbb{Q}$ s.t x< r, z <y.

We first establish the existence of such an r∈ $\mathbb{Q}$. Assume first that x>0. Since 1/(y-x) >0, by Archimedean property, ∃ n∈ $\mathbb{N}$ s.t n>1/(y-x). Hence, ny-nx>1. Since nx>0, by Archimedean property again, ∃ m∈ $\mathbb{N}$ s.t m-1≤ nx <m. Then m≤ nx +1<ny, i.e nx <m<ny. Hence, x<m/n<y and r= m/n ∈ $\mathbb{Q}$. If x=0, then y>0 and by Arichimedean property, ∃ n∈ $\mathbb{N}$ s.t x=0<1/n <y and we simply let r=1/n∈ $\mathbb{Q}$. If x<0 and y>0, then simply let r=0∈ $\mathbb{Q}$. Finally, if x<y≤0, then –x>-y≥0 and we have proved that ∃ r′∈ $\mathbb{Q}$ s.t –x>r′ >-y, i.e x<-r′<y and we let r=-r′∈ $\mathbb{Q}$.

Since $\mathbb{R}\backslash\mathbb{Q}$ is not empty, $\exists$ $z'\in\mathbb{R}\backslash\mathbb{Q}$. By above result, $\exists$ $r\in\mathbb{Q}$ s.t $x+z'<r<y+z'$, i.e $x<r-z'<y$. We claim $z= r-z'\notin\mathbb{Q}$. Suppose not. Then $\exists$ $r'\in\mathbb{Q}$ s.t $r-z'=r'$, i.e $z'=r-r'\in\mathbb{Q}$, a contradiction!

Hence, the density theorem is proven.

Q.E.D

The next chapter employ an approach that aims to extend the Field of Rationals to a Cauchy complete field. If we can show that Dedekind real number systems are also Cauchy complete, then maybe the two approach are not that dissimilar after all. Fortunately, this is indeed the case:

Theorem: Cauchy Completeness of $\mathbb{R}$

Let (x_n) be any sequence in $\mathbb{R}$. Then the following holds:

(i) ***If (x_n) is monotonically increasing and bounded by M, then (x_n) is convergent.***

(ii) ***If (x_n) is monotonically decreasing and bounded by M, then (x_n) is convergent.***

(iii) ***If (x_n) is Cauchy and has a subsequence which converges to x, then we also have $(x_n)\to x$.***

(iv) ***If (x_n) is bounded, $\exists$ a subsequence which is convergent (Bolzano - Weierstrass property)***

(v) ***If (x_n) is Cauchy, it is convergent (Cauchy Completeness).***

(i) Since $|x_n| \le M$ $\forall$ $n\in\mathbb{N}$, the set $A = \{x_n \mid n\in\mathbb{N}\}$ is bounded above by M. Trivially, $x_1\in A$ so $A \neq \phi$. Hence, by order completeness, $x = \text{Sup}A$ exists. Let any $\varepsilon > 0$ be given. Then $\exists$ $x_k\in A$ s.t $x_k > \text{Sup}A - \varepsilon$. Since (x_n) is increasing, we have $x_n \ge x_k$ $\forall$ $n \ge k$. Hence, $\forall$ $n \ge k$,
$\text{Sup}A - \varepsilon < x_k \le x_n \le \text{Sup}A < \text{Sup}A + \varepsilon$
i.e. $|x_n - \text{Sup}A| < \varepsilon$
Hence $(x_n)\to \text{Sup}A$.

(ii) Since $|x_n| \le M$ $\forall$ $n\in\mathbb{N}$, the set $A = \{x_n \mid n\in\mathbb{N}\}$ is bounded below by $-M$. Trivially, $x_1\in A$ so $A \neq \phi$. Then $-A = \{-x_n \mid n\in\mathbb{N}\} \neq \phi$ is bounded above and since $(-x_n)$ is increasing, we have $(-x_n)\to \text{Sup}(-A)$. But $\text{inf}A = -\text{Sup}(-A)$. Since $\lim(-x_n)$ exists, we have

$$\begin{aligned}\lim x_n &= \lim((-1)(-x_n))\\ &= -\lim(-x_n)\\ &= -\text{Sup}(-A)\\ &= -(-\text{inf}A)\\ &= \text{inf}A\end{aligned}$$

i.e. $(x_n)\to \text{inf}A$.

(iii) Let some subsequence $(x_{n(k)})\to x$. Let any $\varepsilon > 0$ be given. Since (x_n) is Cauchy, $\exists$ $N\in\mathbb{N}$ s.t
$|x_n - x_m| < \varepsilon/2 \quad \forall\ n, m \ge N$
Since $(x_{n(k)})\to x$, $\exists$ $T\in\mathbb{N}$ s.t
$|x_{n(k)} - x| < \varepsilon/2 \quad \forall\ k \ge T$
If we take $S = \max(N, T)$, note that $n_S \ge n_N \ge N$.
Hence,

$$\begin{aligned}| x_n - x | &= | (x_n - x_{n(S)}) + (x_{n(S)} - x) | \\ &\leq | x_n - x_{n(S)} | + | x_{n(S)} - x | \\ &< \varepsilon/2 + \varepsilon/2 \qquad \forall\, n \geq N \\ &= \varepsilon \qquad \forall\, n \geq N\end{aligned}$$

Hence, $(x_n) \to x$.

(iv) Now, ∃ a subsequence of (x_n) which is monotone. Since (x_n) is bounded, this subsequence is also bounded. Hence, by (i) and (ii), we can conclude that this subsequence must be convergent.

(v) Now, by (vi), (x_n) has a convergent subsequence. Since (x_n) is also Cauchy, we can conclude, by (iii), that (x_n) is also convergent.

Q.E.D

To show that Dedekind real number systems are indeed unique, it would help if we have the following result at our fingertips:

Theorem:

For any $x, y \in \mathbb{R}$, the following holds:

(i) ***$\{r \mid r \in \mathbb{Q}, r < x + y\} = \{s + t \mid s, t \in \mathbb{Q}, s < x, t < y\}$***

(ii) ***$\{r \mid r \in \mathbb{Q}, 0 < r < xy\} = \{st \mid s, t \in \mathbb{Q}, 0 < s < x, 0 < t < y\}$, $x, y > 0$***

(iii) ***$\mathrm{Sup}\{r \mid r \in \mathbb{Q}, r < x\} = \mathrm{Sup}\{r \mid r \in \mathbb{Q}, 0 < r < x\}$, $x > 0$***

(i) If $s+t \in \{s + t \mid s, t \in \mathbb{Q}, s < x, t < y\}$, then we trivially have $s+ t \in \mathbb{Q}$ and $s+t<x+y$. Hence $\{s + t \mid s, t \in \mathbb{Q}, s < x, t < y\} \subseteq \{r \mid r \in \mathbb{Q}, r < x + y\}$.

Now take $r \in \{r \mid r \in \mathbb{Q}, r < x + y\}$. Then $r - x < y$. By density theorem, $\exists\, r' \in \mathbb{Q}$ s.t $r - x < r' < y$. Then $r - r' < x$. Note that $r - r' \in \mathbb{Q}$ since $r, r' \in \mathbb{Q}$. Hence $r = (r - r') + r' \in \{s + t \mid s, t \in \mathbb{Q}, s < x, t < y\}$

Hence $\{r \mid r \in \mathbb{Q}, r < x + y\} \subseteq \{s + t \mid s, t \in \mathbb{Q}, s < x, t < y\}$.

Hence $\{r \mid r \in \mathbb{Q}, r < x + y\} = \{s + t \mid s, t \in \mathbb{Q}, s < x, t < y\}$.

(ii) Take any $st \in \{st \mid s, t \in \mathbb{Q}, 0 < s < x, 0 < t < y\}$. Then we trivially have $st \in \mathbb{Q}$ and $0 < st < xy$. Hence $\{st \mid s, t \in \mathbb{Q}, 0 < s < x, 0< t< y\} \subseteq \{r \mid r \in \mathbb{Q}, 0< r < xy\}$.

Now take $r \in \{r \mid r \in \mathbb{Q}, 0< r < xy\}$. Then $0 < r/x < y$. By density theorem, $\exists\, r' \in \mathbb{Q}$ s.t $0 < r/x < r' < y$, i.e. $0 < r/ r' < x$. Note that $r/ r' \in \mathbb{Q}$ since $r, r' \in \mathbb{Q}$.

Hence $r = (r/ r')\, r' \in \{s + t \mid s, t \in \mathbb{Q}, 0< s < x, 0 < t < y\}$.

Hence $\{r \mid r \in \mathbb{Q}, 0< r < xy\} \subseteq \{st \mid s, t \in \mathbb{Q}, 0 < s < x, 0 < t < y\}$.

Hence $\{r \mid r \in \mathbb{Q}, 0< r < xy\} = \{st \mid s, t \in \mathbb{Q}, 0 < s < x, 0 < t < y\}$.

(iii) Note first that both sets are bounded above by x so their suprema exists.

Since $\{r \mid r \in \mathbb{Q}, 0 < r < x\} \subseteq \{r \mid r \in \mathbb{Q}, r < x\}$, we have

$\mathrm{Sup}\{r \mid r \in \mathbb{Q}, 0 < r < x\} \leq \mathrm{Sup}\{r \mid r \in \mathbb{Q}, r < x\}$, i.e. $\mathrm{Sup}\{r \mid r \in \mathbb{Q}, r < x\}$ is an upper bound for $\{r \mid r \in \mathbb{Q}, 0<r<x\}$. Now for any $z \in \mathbb{R}$ s.t $z < \mathrm{Sup}\{r \mid r \in \mathbb{Q}, r<x\}$, $\exists\, r' \in \{r \mid r \in \mathbb{Q}, r<x\}$ s.t $z < r'$. If $r'>0$, then simply take $r = r' \in \{r \mid r \in \mathbb{Q}, 0<r<x\}$. Otherwise by density theorem, $\exists\, r \in \mathbb{Q}$ s.t $0 < r< x$ and we still have $z<r' \leq 0<r$.

Hence $\mathrm{Sup}\{r \mid r \in \mathbb{Q}, 0 < r < x\} = \mathrm{Sup}\{r \mid r \in \mathbb{Q}, r < x\}$.

Q.E.D

Finally, we can now show that there is essentially only one Dedekind real number system. The following theorem will wrap up this chapter nicely.

Theorem:

Dedekind real number systems are unique

Consider any 2 Dedekind Real number system $(\mathbb{R}, +, ., >)$ and $(\mathbb{R}', +', .', >')$. By transitivity of isomorphism, $(\mathbb{Q}, +, ., >) \simeq (\mathbb{Q}', +', .', >')$ and we let $\phi: \mathbb{Q} \to \mathbb{Q}'$ be that isomorphism. Define the mapping $\psi: \mathbb{R} \to \mathbb{R}'$ by

$\psi(x) = \text{Sup}A_x \;\; \forall\, x\in \mathbb{R}.$ where $A_x = \{\phi(r) \mid r < x, r\in \mathbb{Q}\}$

We first show that ψ is well-defined. For any $x\in \mathbb{R}$, the Archimedean property for $\mathbb{R}$ demands that $\exists$ $n\in \mathbb{N}$ (hence in $\mathbb{Q}$) s.t $n > x$. Hence, $\phi(r)\in A_x \Rightarrow r<x < n \Rightarrow \phi(r) <' \phi(n)$ (by isomorphism). Hence, A_x is bounded above (by $\phi(n)$) and so by order completeness of $\mathbb{R}'$, $\text{Sup}A_x$ exists, i.e. $\psi(x)\in \mathbb{R}'$. Also, for any $x, y\in \mathbb{R}$ s.t $x = y$, we have

$\psi(x) = \text{Sup}\{\phi(r) \mid r < x, r\in \mathbb{Q}\}$

$= \text{Sup}\{\phi(r) \mid r < x = y, r\in \mathbb{Q}\}$ (note that suprema is unique)

$= \psi(y)$

Hence ψ is well-defined.

Suppose now that $\exists$ $x, y\in \mathbb{R}$ s.t $\psi(x) = \psi(y)$ but $x \neq y$. Without loss of generality, we may assume $x<y$. By density theorem for $\mathbb{R}$, $\exists$ $r_1\in \mathbb{Q}$ s.t $x < r_1 < y$. Applying the density theorem for $\mathbb{R}$ on r_1 and y, we obtain some $r_2\in \mathbb{Q}$ s.t $x < r_1 < r_2 < y$. Now, $\phi(r)\in A_x \Rightarrow r < x < r_1 < r_2 \Rightarrow \phi(r) <' \phi(r_1) <' \phi(r_2)$ (by isomorphism). Hence, both $\phi(r_1)$ and $\phi(r_2)$ are upper bound for A_x. Since $\phi(r_1) <' \phi(r_2)$, we cannot have $\phi(r_2) = \text{Sup}A_x$ and hence $\psi(x) <' \phi(r_2)$. But $\phi(r_2)\in A_y$, so $\psi(x) <' \phi(r_2) \leq' \psi(y)$, contradicting $\psi(x) = \psi(y)$!

Hence ψ must be one-one.

Now take any $x'\in \mathbb{R}'$. Consider the element

$x = \text{Sup}\{r\in \mathbb{Q} \mid \phi(r) <' x'\}$.

We first claim that x exists, i.e. $x\in \mathbb{R}$. By Archimedean property for $\mathbb{R}'$, $\exists$ $n'\in \mathbb{N}'$ (hence in $\mathbb{Q}'$) s.t $n' >' x'$. As ϕ is onto, $\exists$ $n\in \mathbb{Q}$ s.t $n' = \phi(n)$. Then $\phi(r) <' x' \Rightarrow \phi(r) <' x' <' \phi(n) \Rightarrow r < n$ (by isomorphism). Hence n is an upper bound for $\{r\in \mathbb{Q} \mid \phi(r) <' x'\}$ and so by order completeness of $\mathbb{R}$, x exists.

Now, we want to claim that $\text{Sup}A_x = x'$. If x' is not an upper bound for A_x, then $\exists$ $\phi(r)\in A_x$ s.t $\phi(r) >' x'$. Then $r\notin \{r\in \mathbb{Q} \mid \phi(r) <' x'\}$. Since $r < x$, r is not an upper bound for $\{r\in \mathbb{Q} \mid \phi(r) <' x'\}$ and so $\exists$ $r_1\in \{r\in \mathbb{Q} \mid \phi(r) <' x'\}$ s.t $r < r_1$. By isomorphism, $\phi(r) <' \phi(r_1)$, i.e. $\phi(r) <' \phi(r_1) <' x'$ and so $r\in \{r\in \mathbb{Q} \mid \phi(r) <' x'\}$, a contradiction! Hence x' is an upper bound for A_x. Now take any $y'\in \mathbb{R}'$ s.t $y' <' x'$. Then by density theorem for $\mathbb{R}'$, $\exists$ $r_1'\in \mathbb{Q}'$ s.t $y' <' r_1' <' x'$. Applying the density theorem on r_1' and x', we obtain $r_2'\in \mathbb{Q}'$ s.t $y' <' r_1' <' r_2' <' x'$. Since ϕ is onto, $\exists$ $r_1, r_2\in \mathbb{Q}$ s.t $\phi(r_1)=r_1'$, $\phi(r_2) = r_2'$, i.e. $r_1, r_2\in \{r\in \mathbb{Q} \mid \phi(r) <' x'\}$ and so $r_1, r_2 \leq x$. By isomorphism, $\phi(r_1)<' \phi(r_2)$

$\Rightarrow r_1 < r_2$ and so we have $r_1 < x$. Then $r_1' = \phi(r_1) \in A_x$ and $y' <' r_1' <' x'$. Hence $x' = \text{Sup}A_x$, i.e. $\psi(x) = x'$.

Hence ψ is onto.

Take any $x, y \in \mathbb{R}$.

(i)
$$\begin{aligned}
\psi(x + y) &= \text{Sup}\{\phi(r) \mid r < x + y, r \in \mathbb{Q}\} \\
&= \text{Sup}\{\phi(s + t) \mid s < x,\ t < y, s, t \in \mathbb{Q}\} \\
&= \text{Sup}\{\phi(s) +' \phi(t) \mid s < x,\ t < y, s, t \in \mathbb{Q}\} \text{ (by isomorphism)} \\
&= \text{Sup}\{\phi(s) \mid s < x, s \in \mathbb{Q}\} +' \text{Sup}\{\phi(t) \mid t < y, t \in \mathbb{Q}\} \\
&= \psi(x) +' \psi(y).
\end{aligned}$$

(ii) Assume first that $x, y > 0$. Then

$$\begin{aligned}
\psi(x.y) &= \text{Sup}\{\phi(r) \mid r < x.y, r \in \mathbb{Q}\} \\
&= \text{Sup}\{\phi(r) \mid 0 < r < x.y, r \in \mathbb{Q}\} \\
&= \text{Sup}\{\phi(s.t) \mid 0 < s < x, 0 < t < y, s, t \in \mathbb{Q}\} \\
&= \text{Sup}\{\phi(s) .' \phi(t) \mid 0 < s < x, 0 < t < y, s, t \in \mathbb{Q}\} \text{ (by isomorphism)} \\
&= \text{Sup}\{\phi(s) \mid 0 < s < x, s \in \mathbb{Q}\} .' \text{Sup}\{\phi(t) \mid 0 < t < y, t \in \mathbb{Q}\} \text{(note that by isomorphism, } \phi(s), \phi(t) >' 0') \\
&= \text{Sup}\{\phi(s) \mid s < x, s \in \mathbb{Q}\} .' \text{Sup}\{\phi(t) \mid t < y, t \in \mathbb{Q}\} \\
&= \psi(x) .' \psi(y).
\end{aligned}$$

Before we consider the subcases, we establish 2 results:

First, we claim $\psi(0) = 0'$. Now for $r \in \mathbb{Q}$, $r < 0 \Rightarrow \phi(r) <' \phi(0)$ by isomorphism. Hence $\phi(0)$ is an upper bound for A_0. Let $z' \in \mathbb{R}'$ be s.t $z' <' \phi(0)$. By density theorem for $\mathbb{R}'$, $\exists\ r' \in \mathbb{Q}'$ s.t $z' <' r' <' \phi(0)$. By onto nature of ϕ, $\exists\ r \in \mathbb{Q}$ s.t $\phi(r) = r'$. By isomorphism $r < 0$ and so $\phi(r) \in A_0$ and $\phi(r) <' \phi(0)$. Hence, $\phi(0) = \text{Sup}A_0 = \psi(0)$. By isomorphism, $\phi(0) = 0'$ and so $\psi(0) = 0'$.

Also, we claim $\psi(-x) = -\psi(x)\ \forall\ x \in \mathbb{R}$. Now

$$\begin{aligned}
0' = \psi(0) &= \psi(x + (-x)) \\
&= \psi(x) +' \psi(-x) \quad \text{(by (i))}
\end{aligned}$$

i.e. $\psi(-x) = -\psi(x)$.

We are now ready to consider the subcases.

(a) One of x, y is zero.

Without loss of generality (due to commutativity), we may assume $x = 0$. Then

$$\begin{aligned}
\psi(x.y) &= \psi(0.y) \\
&= \psi(0) \\
&= 0' \\
&= 0' .' \psi(y) \\
&= \psi(x) .' \psi(y)
\end{aligned}$$

(b) $x, y < 0$

$$\begin{aligned}
\psi(x.y) &= \psi((-x).(-y)) \\
&= \psi(-x) .' \psi(-y) \qquad (\because -x, -y > 0) \\
&= (-\psi(x)) .' (-\psi(y)) \\
&= \psi(x) .' \psi(y)
\end{aligned}$$

(c) $x > 0, y < 0$

$$\begin{aligned} -\psi(x.y) &= \psi(-(x.y)) \\ &= \psi(x.(-y)) \\ &= \psi(x) .' \psi(-y) \quad (\because x, -y > 0) \\ &= \psi(x) .' (-\psi(y)) \\ &= -(\psi(x) .' \psi(y)) \end{aligned}$$

i.e. $\psi(x.y) = \psi(x) .' \psi(y)$

(d) $x < 0, y > 0$

By symmetry, (due to commutativity), this follows from (c).

Hence $\psi(x.y) = \psi(x) .' \psi(y)$

(iii) Suppose $x < y$. Then by density theorem for $\mathbb{R}$, $\exists\, r_1 \in \mathbb{Q}$ s.t $x < r_1 < y$. Applying the density theorem for $\mathbb{R}$ on r_1 and y, we obtain $r_2 \in \mathbb{Q}$ s.t $x < r_1 < r_2 < y$. Now, for $r \in \mathbb{Q}$, $r < x \Rightarrow r < r_1 < r_2 \Rightarrow \phi(r) <' \phi(r_1) <' \phi(r_2)$ by isomorphism. Hence both $\phi(r_1)$ and $\phi(r_2)$ are upper bound for A_x. Also $\phi(r_2) \neq \text{Sup}A_x$ since $\phi(r_1) <' \phi(r_2)$. Hence $\text{Sup}A_x <' \phi(r_2)$. Also, we trivially have $\phi(r_2) \in A_y$ so $\phi(r_2) \leq' \text{Sup}A_y$. Hence, $\text{Sup}A_x <' \phi(r_2) \leq' \text{Sup}A_y$, i.e. $\psi(x) <' \psi(y)$.

Hence, ψ is an isomorphism from $(\mathbb{R}, +, ., >)$ to $(\mathbb{R}', +', .', >')$ and so $(\mathbb{R}, +, ., >) \simeq (\mathbb{R}', +', .', >')$.

Q.E.D

Let us now turn to Cantor's approach and see what he has to offer. Perhaps his real number system may be more desirable...

End Of Chapter 4.1

CHAPTER 4.2: CANTOR REAL NUMBER SYSTEM

Cantor's Approach

Defn: Let $\mathcal{C}$ denote the set of all Cauchy sequences in $\mathbb{Q}$. We say (r_n), $(s_n) \in \mathcal{C}$ are equivalent and we write $(r_n) \sim (s_n)$ if given any rational $\varepsilon > 0$, $\exists\ k \in \mathbb{N}$ such that $| r_n - s_n | < \varepsilon \quad \forall\ n \geq k$.

Cantor believed that on the real number line, any Cauchy sequences should converge to some point. Of course, he cannot technically use real Cauchy sequences, so he looked instead at the next best thing: the set of all rational Cauchy sequences $\mathcal{C}$. If we presuppose knowledge of the real number system, we know that for any real number, there exist a rational sequence that converges to that point. Since a convergent sequence is necessarily Cauchy, we are now at least assured that Cantor's Approach will 'pinpoint' all the gaps. The technical definition given above should now be easy to understand. Two related sequences in the definition have terms that are eventually very close to each other, and so we should expect the two sequences to converge to the same point, whether it be a rational point or a gap.

The following theorem tells us that our partition is indeed an equivalence relation, which we certainly hope to be the case.

Theorem:

The relation $\sim$ is an equivalence relation on $\mathcal{C}$

Take any $(r_n) \in \mathcal{C}$. Given any $\varepsilon > 0$, take $1 \in \mathbb{N}$. Then

$| r_n - r_n | = 0 < \varepsilon \qquad \forall\ n \geq 1$

Hence, $(r_n) \sim (r_n)$. Hence $\sim$ is reflesive.

Take any (r_n), $(s_n) \in \mathcal{C}$ s.t $(r_n) \sim (s_n)$. Given any $\varepsilon > 0$, $\exists\ k \in \mathbb{N}$ s.t

$| r_n - s_n | < \varepsilon \qquad \forall\ n \geq k$

i.e. $| s_n - r_n | = | r_n - s_n | < \varepsilon \qquad \forall\ n \geq k$

Hence, $(s_n) \sim (r_n)$. Hence, $\sim$ is symmetric.

Take any (r_n), (s_n), $(t_n) \in \mathcal{C}$ s.t $(r_n) \sim (s_n)$ and $(s_n) \sim (t_n)$. Then given any $\varepsilon > 0$, $\exists\ k_1, k_2 \in \mathbb{N}$ s.t

$| r_n - s_n | < \varepsilon/2 \quad \forall\ n \geq k_1 \qquad | s_n - t_n | < \varepsilon/2 \quad \forall\ n \geq k_2$.

Take $k = \max(k_1, k_2)$. Then

$| r_n - s_n | < \varepsilon/2,\ | s_n - t_n | < \varepsilon/2 \qquad \forall\ n \geq k$.

$$\begin{aligned} \text{But } | r_n - t_n | &= | (r_n - s_n) + (s_n - t_n) | \\ &\leq | r_n - s_n | + | s_n - t_n | \\ &< \varepsilon/2 + \varepsilon/2 \qquad \forall\ n \geq k \\ &= \varepsilon \qquad \forall\ n \geq k \end{aligned}$$

Hence, $(r_n) \sim (t_n)$. Hence, $\sim$ is transitive.

Hence, $\sim$ is an equivalence relation on $\mathcal{C}$.

Q.E.D

We will denote $\mathcal{C}/\sim$ by $\mathbb{R}$. An element $x \in \mathbb{R}$ will be aptly called a x-convergence point. The next theorem gives us technical evidence that our intuition that each equivalence class actually represent the same point of convergence for the sequences in that class is correct, at least when we restrict ourselves to rational convergence points.

Theorem: Rational Convergence Point

Let $(r_n) \in \mathcal{C}$ be s.t $(r_n) \to r \in \mathbb{Q}$. Then $(r_n) \sim (s_n)$ iff $(s_n) \to r$. We call $[(r_n)]$ a rational convergence point. In this case, we denote $[(r_n)]$ simply as $[r]$.

Suppose $(r_n) \sim (s_n)$. Let any $\varepsilon > 0$ be given. Then $\exists\, k_1 \in \mathbb{N}$ s.t
$| r_n - s_n | < \varepsilon/2 \quad \forall\, n \geq k_1$

Since $(r_n) \to r$, $\exists\, k_2 \in \mathbb{N}$ s.t
$| r_n - r | < \varepsilon/2 \quad \forall\, n \geq k_2$

Take $k = \max(k_1, k_2)$ and we have
$| r_n - s_n | < \varepsilon/2, | r_n - r | < \varepsilon/2 \quad \forall\, n \geq k.$
But

$$\begin{aligned} | s_n - r | &= | (s_n - r_n) + (r_n - r) | \\ &\leq | s_n - r_n | + | r_n - r | \\ &< \varepsilon/2 + \varepsilon/2 && \forall\, n \geq k \\ &= \varepsilon && \forall\, n \geq k. \end{aligned}$$

Hence, $(s_n) \to r$.

Now suppose $(s_n) \to r$. Note that this means $(s_n) \in \mathcal{C}$. Then given $\varepsilon > 0$, $\exists\, k_1 \in \mathbb{N}$ s.t
$| s_n - r | < \varepsilon/2 \quad \forall\, n \geq k_1$

Since $(r_n) \to r$, $\exists\, k_2 \in \mathbb{N}$ s.t
$| r_n - r | < \varepsilon/2 \quad \forall\, n \geq k_2$

Take $k = \max(k_1, k_2)$ and we have
$| r_n - r | < \varepsilon/2, \ | s_n - r | < \varepsilon/2 \quad \forall\, n \geq k.$
But

$$\begin{aligned} | r_n - s_n | &= | (r_n - r) + (r - s_n) | \\ &\leq | r_n - r | + | r - s_n | \\ &< \varepsilon/2 + \varepsilon/2 && \forall\, n \geq k \\ &= \varepsilon && \forall\, n \geq k. \end{aligned}$$

Hence $(r_n) \sim (s_n)$.

Q.E.D

For any $r \in \mathbb{Q}$, we hence will have the constant sequence $r_n = r \ \forall\, n \in \mathbb{N}$ belonging to $[r]$. We will denote this constant sequence simply as (r). We call the set of all rational convergence point as $\mathbb{R}_{\mathbb{Q}}$, since it is supposed to represent our copy of the rationals in this new system.

Binary Operation on $\mathbb{R}$

Let us now define appropriate binary operations on our new system to make it a field.

Theorem: Addition on $\mathbb{R}$

$\exists$ a well-defined binary operation $\oplus$ on $\mathbb{R}$ given by

$[(r_n)] \oplus [(s_n)] = [(r_n + s_n)]$ $\forall [(r_n)], [(s_n)] \in \mathbb{R}$.

First note that $(r_n), (s_n) \in \mathcal{C} \Rightarrow (r_n + s_n) \in \mathcal{C}$. Hence, $[(r_n + s_n)] \in \mathbb{R}$.

Let $[(r_n)] = [(r_n')]$ and $[(s_n)] = [(s_n')]$. Then $(r_n) \sim (r_n')$ and $(s_n) \sim (s_n')$. Given any $\varepsilon > 0$, $\exists$ $k_1, k_2 \in \mathbb{N}$ s.t

$| r_n - r_n' | < \varepsilon/2 \quad \forall n \geq k_1$

$| s_n - s_n' | < \varepsilon/2 \quad \forall n \geq k_2$

Take $k = \max(k_1, k_2)$ and we have

$| r_n - r_n' | < \varepsilon/2, | s_n - s_n' | < \varepsilon/2 \quad \forall n \geq k$

But

$$\begin{aligned} | (r_n + s_n) - (r_n' + s_n') | &= | (r_n - r_n') + (s_n - s_n') | \\ &\leq | r_n - r_n' | + | s_n - s_n' | \\ &< \varepsilon/2 + \varepsilon/2 \quad \forall n \geq k \\ &= \varepsilon \quad \forall n \geq k \end{aligned}$$

i.e. $(r_n + s_n) \sim (r_n' + s_n')$.

Hence, $[(r_n)] \oplus [(s_n)] = [(r_n')] \oplus [(s_n')]$.

Hence, $\oplus$ is well-defined.

Q.E.D

<u>Theorem: Properties of addition on $\mathbb{R}$</u>

$\forall [(r_n)], [(s_n)], [(t_n)] \in \mathbb{R}$, we have

$A_{\mathbb{R}}$(i) $[(r_n)] \oplus [(s_n)] = [(s_n)] \oplus [(r_n)]$

$$\begin{aligned} [(r_n)] \oplus [(s_n)] &= [(r_n + s_n)] \\ &= [(s_n + r_n)] \\ &= [(s_n)] \oplus [(r_n)] \end{aligned}$$

$A_{\mathbb{R}}$(ii) $([(r_n)] \oplus [(s_n)]) \oplus [(t_n)] = [(r_n)] \oplus ([(s_n)] \oplus [(t_n)])$

$$\begin{aligned} ([(r_n)] \oplus [(s_n)]) \oplus [(t_n)] &= [(r_n + s_n)] \oplus [(t_n)] \\ &= [((r_n + s_n) + t_n)] \\ &= [(r_n + (s_n + t_n))] \\ &= [(r_n)] \oplus [(s_n + t_n)] \\ &= [(r_n)] \oplus ([(s_n)] \oplus [(t_n)]) \end{aligned}$$

$A_{\mathbb{R}}$(iii) The $\oplus$-identity exists and is given by [0].

$$\begin{aligned} [(r_n)] \oplus [0] &= [(r_n)] \oplus [(0)] \\ &= [(r_n + 0)] \\ &= [(r_n)] \end{aligned}$$

Together with $A_{\mathbb{R}}$(i), we have $[(r_n)] \oplus [0] = [(r_n)] = [0] \oplus [(r_n)]$

$A_{\mathbb{R}}$(iv) For any $[(r_n)]$, its $\oplus$-inverse exists and is given by $[(-r_n)]$

$$\begin{aligned} [(r_n)] \oplus [(-r_n)] &= [(r_n + (-r_n))] \\ &= [(0)] \\ &= [0] \end{aligned}$$

Together with $A_{\mathbb{R}}$(i), we have $[(r_n)] \oplus [(-r_n)] = [0] = [(-r_n)] \oplus [(r_n)]$

Q.E.D

This makes $(\mathbb{R}, \oplus)$ a commutative group.

Theorem: Multiplication on $\mathbb{R}$

$\exists$ a well-defined binary operation $\odot$ on $\mathbb{R}$ given by

$[(r_n)] \odot [(s_n)] = [(r_n s_n)] \qquad \forall [(r_n)], [(s_n)] \in \mathbb{R}$.

First, note that $(r_n), (s_n) \in \mathcal{C} \Rightarrow (r_n s_n) \in \mathcal{C}$. Hence $[(r_n s_n)] \in \mathbb{R}$.

Let $[(r_n)] = [(r_n')]$ and $[(s_n)] = [(s_n')]$. Then $(r_n) \sim (r_n')$ and $(s_n) \sim (s_n')$. Note that since (r_n) and (s_n') is Cauchy, they are bounded by some R and S′ respectively. Given any $\varepsilon > 0$, $\exists\, k_1, k_2 \in \mathbb{N}$ s.t

$| r_n - r_n' | < \varepsilon/(2S') \qquad \forall\, n \geq k_1$

$| s_n - s_n' | < \varepsilon/(2R) \qquad \forall\, n \geq k_2$

Take $k = \max(k_1, k_2)$ and we have

$| r_n - r_n' | < \varepsilon/(2S'), \quad | s_n - s_n' | < \varepsilon/(2R) \qquad \forall\, n \geq k$

But

$$\begin{aligned}
| r_n s_n - r_n' s_n' | &= | (r_n s_n - r_n s_n') + (r_n s_n' - r_n' s_n') | \\
&\leq | r_n s_n - r_n s_n' | + | r_n s_n' - r_n' s_n' | \\
&= | r_n | \, | s_n - s_n' | + | s_n' | \, | r_n - r_n' | \\
&\leq R\, | s_n - s_n' | + S'\, | r_n - r_n' | \\
&< R(\varepsilon/(2R)) + S'(\varepsilon/(2S')) \qquad \forall\, n \geq k \\
&= \varepsilon \qquad \forall\, n \geq k
\end{aligned}$$

i.e. $(r_n s_n) \sim (r_n' s_n')$.

Hence, $[(r_n)] \odot [(s_n)] = [(r_n')] \odot [(s_n')]$

Hence, $\odot$ is well-defined.

Q.E.D

Properties of multiplication on $\mathbb{R}$

$M_{\mathbb{R}}$(i) $[(r_n)] \odot [(s_n)] = [(s_n)] \odot [(r_n)]$

$$\begin{aligned}
[(r_n)] \odot [(s_n)] &= [(r_n s_n)] \\
&= [(s_n r_n)] \\
&= [(s_n)] \odot [(r_n)]
\end{aligned}$$

$M_{\mathbb{R}}$(ii) $([(r_n)] \odot [(s_n)]) \odot [(t_n)] = [(r_n)] \odot ([(s_n)] \odot [(t_n)])$

$$\begin{aligned}
([(r_n)] \odot [(s_n)]) \odot [(t_n)] &= [(r_n s_n)] \odot [(t_n)] \\
&= [((r_n s_n) t_n)] \\
&= [(r_n (s_n t_n))] \\
&= [(r_n)] \odot [(s_n t_n)] \\
&= [(r_n)] \odot ([(s_n)] \odot [(t_n)])
\end{aligned}$$

$M_{\mathbb{R}}$(iii) The identity element exist and is given by [1].

$$\begin{aligned}
[(r_n)] \odot [1] &= [(r_n)] \odot [(1)] \\
&= [(r_n 1)] \\
&= [(r_n)]
\end{aligned}$$

Together with $M_{\mathbb{R}}$(i), we have $[(r_n)] \odot [1] = [(r_n)] = [1] \odot [(r_n)]$

$M_{\mathbb{R}}$(iv) If $[(r_n)]\neq[0]$, then its $\odot$–inverse exist.

Since $[(r_n)]\neq[0]$, we cannot have $(r_n)\to 0$. Hence, $\exists$ a k-tail of (r_n), i.e (r_{n+k-1}), s.t $(1/r_{n+k-1})$ is well defined (i.e $r_{n+k-1}\neq 0\ \forall\ n\in\mathbb{N}$) and Cauchy. Define the sequence (s_n) by

$$s_n = \begin{cases} 0 & \text{if } n<k \\ 1/r_n & \text{if } n\geq k \end{cases}$$

Also, define the sequence (t_n) by

$$t_n = \begin{cases} 0 & \text{if } n<k \\ 1 & \text{if } n\geq k \end{cases}$$

As $(t_n)\to 1$, we have $(t_n) \sim (1)$. Also, since the k-tail of (s_n) is the sequence $(1/r_{n+k-1})$ which is Cauchy, we will also have (s_n) Cauchy and hence $[(s_n)]\in\mathbb{R}$. Now,

$$\begin{aligned}[(r_n)] \odot [(s_n)] &=[(r_n s_n)] \\ &=[(t_n)] \\ &=[1]\end{aligned}$$

Together with $M_{\mathbb{R}}$(i), we have $[(r_n)] \odot [(s_n)] =[1] =[(s_n)] \odot [(r_n)]$.

$M_{\mathbb{R}}$(v) $[(r_n)] \odot ([(s_n)] \oplus [(t_n)]) = ([(r_n)] \odot[(s_n)]) \oplus ([(r_n)] \odot [(t_n)])$

$$\begin{aligned}[(r_n)] \odot ([(s_n)] \oplus [(t_n)]) &=[(r_n)] \odot [(s_n + t_n)] \\ &=[(r_n(s_n + t_n))] \\ &=[(r_n s_n + r_n t_n)]\end{aligned}$$

$$\begin{aligned}([(r_n)] \odot[(s_n)]) \oplus ([(r_n)] \odot [(t_n)]) &= [(r_n s_n)] \oplus [(r_n t_n)] \\ &= [(r_n s_n + r_n t_n)] \\ &= [(r_n)] \odot ([(s_n)] \oplus [(t_n)])\end{aligned}$$

Q.E.D

Hence, this makes $(\mathbb{R}, \oplus, \odot)$ a field. We still need to define an appropriate order so that this system is 'complete'. Let us proceed then to the next section to do this.

Order on $\mathbb{R}$

Before we define our subset of 'positive elements', we need first to define the concept of a positive sequence. The following definition may be a bit misleading to some readers who might mistook a positive sequence to mean a sequence that have all its terms positive eventually. Hence, they might wonder why we use a positive rational r instead of 0 which should work equally well. Well, a positive sequence in $\mathcal{C}$ certainly will be a sequence with positive terms eventually but the definition really intend a sequence in $\mathcal{C}$ that will converge to a positive point. Hence, if we use 0, we will include sequences that converges to 0! Let us define positive sequences now formally.

Defn: For any $(r_n)\in\mathcal{C}$, we say that (r_n) is a positive sequence if $\exists$ some rational $r>0$ and a $k\in\mathbb{N}$ such that $r_n > r\ \ \forall\ n\geq k$

The above definition makes our choice of $P_{\mathbb{R}}$ obvious:

Defn: We define the subset $P_{\mathbb{R}}$ of $\mathbb{R}$ by

$P_{\mathbb{R}} =\{ [(r_n)] \in \mathbb{R} | (r_n)$ is a positive sequence $\}$

<u>Theorem:</u>

The set $P_{\mathbb{R}}$ is a well-defined set.

Let $[(r_n)]\in P_{\mathbb{R}}$. We must show that if $(s_n) \sim (r_n)$, then $[(s_n)]\in P_{\mathbb{R}}$ also, i.e (s_n) is a positive sequence.

Since (r_n) is a positive sequence, $\exists$ some rational $r>0$ and a $k_1\in \mathbb{N}$ s.t
$r_n > r \ \forall \ n\geq k_1$

Also, as $(s_n) \sim (r_n)$, for $\varepsilon = r/2 >0$, $\exists$ $k_2\in \mathbb{N}$ s.t
$| r_n - s_n | < r/2 \quad \forall \ n \geq k_2$
Take $k= \max(k_1,k_2)$. Then $\forall$ $n \geq k$, we have
$| r_n - s_n | < r/2 , \quad r_n > r$
$\Rightarrow r_n - s_n < r/2 , \quad r_n > r$
$\Rightarrow r- r/2 < r_n - r/2 < s_n$, i.e $0< r/2< s_n$
Hence, (s_n) is also a positive sequence.

Hence, $P_{\mathbb{R}}$ is a well-defined set.
Q.E.D

The next theorem tells us that $P_{\mathbb{R}}$ is indeed the set of 'positive' elements.

<u>Theorem:</u>

For any $[(r_n)]\in \mathbb{R}$, one and only one of the following holds:

$[(r_n)]=[0]$, $[(r_n)]\in P_{\mathbb{R}}$, $-[(r_n)]\in P_{\mathbb{R}}$.

Furthermore, $P_{\mathbb{R}}$ is closed under $\oplus$ and $\odot$.

Take any $[(r_n)]\in \mathbb{R}$. We first show that one of the cases must hold. If $[(r_n)]\neq[0]$, then we cannot have $(r_n)\to 0$. Hence, $\exists$ a rational $r>0$ and a $k_1\in \mathbb{N}$ s.t
$| r_n|\geq r \ \forall \ n\geq k_1$

For $\varepsilon = r/2 > 0$, $\exists$ $k_2\in \mathbb{N}$ s.t
$| r_n - r_m | < r/2 \ \forall \ n, m \geq k_2$
Take $k = \max(k_1, k_2)$. Then we have
$| r_n|\geq r \qquad | r_n - r_m | < r/2 \ \forall \ n, m \geq k$
In particular, we have
$| r_k|\geq r \qquad | r_n - r_k | < r/2 \ \forall \ n \geq k$
Hence, $\forall$ $n \geq k$, we have
$-(r/2) < r_n - r_k < r/2$
$r_k - r/2 < r_n < r_k + r/2$
Since $| r_k|\geq r$, there are only 2 cases:
(a) $r_k \geq r$
Then $r/2 = r - r/2 \leq r_k - r/2 < r_n$

This means $r_n > r/2 \ \forall \ n \geq k$ and so (r_n) is a positive sequence, i.e. $[(r_n)]\in P_{\mathbb{R}}$.
(b) $r_k \leq -r$
Then $r_n < r_k + r/2 \leq -r + r/2 = -(r/2)$

This means $-r_n > r/2 \ \forall\ n \geq k$ and so $(-r_n)$ is a positive sequence. Hence, $-[(r_n)] = [(-r_n)] \in P_{\mathbb{R}}$.

Hence, one of the cases must hold.

If $[(r_n)] \in P_{\mathbb{R}}$, then $\exists\ r > 0$, $k \in \mathbb{N}$ s.t
$r_n > r \ \forall\ n \geq k$

i.e. $-r_n < -r < 0 \ \forall\ n \geq k$ and hence it is impossible that $-[(r_n)] = [(-r_n)] \in P_{\mathbb{R}}$.

By symmetry, we may claim that $[(r_n)] \in P_{\mathbb{R}}$ and $-[(r_n)] \in P_{\mathbb{R}}$ never hold together.

If $[(r_n)] = [0]$, then $(r_n) \to 0$. Hence, for any rational $r > 0$, $\exists\ k \in \mathbb{N}$ s.t
$| r_n | < r \ \forall\ n \geq k$

i.e. $r_n \leq | r_n | < r \ \forall\ n \geq k$ and hence it is impossible that $[(r_n)] \in P_{\mathbb{R}}$

Hence $[(r_n)] = [0]$ and $[(r_n)] \in P_{\mathbb{R}}$ never hold together.

Since $[(r_n)] = [0] \Leftrightarrow -[(r_n)] = [0]$, we may claim from preceding result that $[(r_n)] = [0]$ and $-[(r_n)] \in P_{\mathbb{R}}$ never hold together also.

Hence, one and only one of the cases is true.

Take any $[(r_n)]$, $[(s_n)] \in P_{\mathbb{R}}$. Then $\exists$ rationals $r, s > 0$ s.t $\exists\ k_1, k_2 \in \mathbb{N}$ where
$r_n > r > 0 \ \forall\ n \geq k_1$
$s_n > s > 0 \ \forall\ n \geq k_2$

Take $k = \max(k_1, k_2)$ and we have
$r_n > r > 0, \qquad s_n > s > 0 \ \forall\ n \geq k$

i.e. $r_n + s_n > r + s > 0$, $r_n s_n > rs > 0 \ \forall\ n \geq k$

Hence, $(r_n + s_n)$, $(r_n s_n)$ are both positive sequence. Then

$[(r_n)] \oplus [(s_n)] = [(r_n + s_n)] \in P_{\mathbb{R}}$.

$[(r_n)] \odot [(s_n)] = [(r_n s_n)] \in P_{\mathbb{R}}$.

Hence, $P_{\mathbb{R}}$ is closed under $\oplus$ and $\odot$.

Q.E.D

The following definition will then make our field ordered.

Defn: We say that $[(r_n)]$ is greater than $[(s_n)]$ and we write $[(r_n)] \succ [(s_n)]$ if $[(r_n)] \oplus (-[(s_n)]) \in P_{\mathbb{R}}$. We write $[(r_n)] \succcurlyeq [(s_n)]$ if $[(r_n)] \succ [(s_n)]$ or $[(r_n)] = [(s_n)]$.

Hence, $(\mathbb{R}, \oplus, \odot, \succ)$ is an ordered field. The following result tells us what this order means explicitly in our new system.

Theorem:

$[(r_n)] \succ [(s_n)]$ iff $(r_n - s_n)$ is a positive sequence.

We have

$$[(r_n)] \succ [(s_n)] \Leftrightarrow [(r_n)] \oplus (-[(s_n)]) \in P_{\mathbb{R}}.$$
$$\Leftrightarrow [(r_n - s_n)] \in P_{\mathbb{R}}.$$
$$\Leftrightarrow (r_n - s_n) \text{ is a positive sequence.}$$

Q.E.D

The Cantor Real Number System

Before we give a formal definition of a Cantor Real Number System, let us first show that our new system contain a copy of the rationals.

Theorem:

($\mathbb{R}_{\mathbb{Q}}$, $\oplus$, $\odot$, $\succ$) is a subfield of ($\mathbb{R}$, $\oplus$, $\odot$, $\succ$). Furthermore,

($\mathbb{R}_{\mathbb{Q}}$, $\oplus$, $\odot$, $\succ$) $\simeq$ ($\mathbb{Q}$, +, ., >).

Take any [r], [s]$\in$ $\mathbb{R}_{\mathbb{Q}}$. Then

$$\begin{aligned}[r] \oplus (-[s]) &= [(r)] \oplus (-[(s)]) \\ &= [(r)] \oplus [(-s)] \\ &= [(r-s)] \\ &= [r-s] \ (\in \mathbb{R}_{\mathbb{Q}})\end{aligned}$$

$$\begin{aligned}[r] \odot ([s])^{-1} &= [(r)] \odot ([(s)])^{-1} \\ &= [(r)] \odot [(1/s)] \ \forall\ [s] \neq [0], \text{ note this means } s \neq 0 \\ &= [(r/s)] \\ &= [r/s] \ (\in \mathbb{R}_{\mathbb{Q}})\end{aligned}$$

Obviously, [1]$\in \mathbb{R}_{\mathbb{Q}}$. Hence ($\mathbb{R}_{\mathbb{Q}}$, $\oplus$, $\odot$, $\succ$) is a subfield of ($\mathbb{R}$, $\oplus$, $\odot$, $\succ$).

Consider the mapping $\phi:\mathbb{R}_{\mathbb{Q}} \to \mathbb{Q}$ given by

$\phi([r]) = r\ \forall\ [r]\in \mathbb{R}_{\mathbb{Q}}$.

$[r_1] = [r_2] \Rightarrow \lim(r_1) = \lim(r_2) \Rightarrow r_1 = r_2$. Hence, ϕ is well-defined.

Let $r_1 = r_2$. Then $\lim(r_1) = \lim(r_2)$ and so $(r_1) \sim (r_2)$, i.e. $[r_1] = [r_2]$. Hence, ϕ is one – one.

For any r$\in \mathbb{Q}$, take [r]$\in \mathbb{R}_{\mathbb{Q}}$ and we will have $\phi([r]) = r$. Hence ϕ is onto.

Hence ϕ is bijective.

For any [r], [s]$\in \mathbb{R}_{\mathbb{Q}}$,

$$\begin{aligned}\phi([r] \oplus [s]) &= \phi(\ [(r)] \oplus [(s)]\ ) \\ &= \phi(\ [(r+s)]\ ) \\ &= \phi([r+s]) \\ &= r+s \\ &= \phi([r]) + \phi([s])\end{aligned}$$

$$\begin{aligned}\phi([r] \odot [s]) &= \phi(\ [(r)] \odot [(s)]\ ) \\ &= \phi(\ [(r.s)]\ ) \\ &= \phi([r.s]) \\ &= r.s \\ &= \phi([r]).\phi([s])\end{aligned}$$

$$\begin{aligned}[r] \succ [s] &\Rightarrow [(r)] \succ [(s)] \\ &\Rightarrow (r-s) \text{ is a positive sequence} \\ &\Rightarrow r_n - s_n > t\ \forall\ n \geq k \text{ for some } t\in \mathbb{Q},\ t > 0,\ k\in \mathbb{N} \\ &\Rightarrow r - s > t \text{ since } r_n = r,\ s_n = s\ \forall\ n\in \mathbb{N} \\ &\Rightarrow r > t + s, \text{ i.e. } r > s \text{ since } t > 0\end{aligned}$$

Hence ϕ is an isomorphism from $\mathbb{R}_{\mathbb{Q}}$ to $\mathbb{Q}$ and so ($\mathbb{R}_{\mathbb{Q}}$, $\oplus$, $\odot$, $\succ$) $\simeq$ ($\mathbb{Q}$, +, ., >).

Q.E.D

The next result is a weakened form of the density theorem in the familar real number system. But it is nonetheless sufficient for the remainder of the results that we are going to prove.

Theorem: Denseness of rationals

Let $[(s_n)], [(t_n)]\in\mathbb{R}$ be s.t $[(s_n)] \prec [(t_n)]$. Then $\exists\, [r]\in\mathbb{R}_{\mathbb{Q}}$ s.t $[(s_n)] \prec [r] \prec [(t_n)]$.

Since $[(s_n)] \prec [(t_n)]$, $(t_n - s_n)$ is a positive sequence and so $\exists$ a rational $r' > 0$ and a $k_1\in\mathbb{N}$ s.t

$t_n - s_n > r' \ \forall\, n \geq k_1$

As (s_n), (t_n) are Cauchy, $\exists\, k_2, k_3\in\mathbb{N}$ s.t

$| t_n - t_m | < r'/3 \quad \forall\, n, m \geq k_2$

$| s_n - s_m | < r'/3 \quad \forall\, n, m \geq k_3$

Take $k = \max(k_1, k_2, k_3)$ and we have, $\forall\, n \geq k$,

$$| t_n - t_k | < r'/3 \qquad | s_n - s_k | < r'/3 \qquad t_n - s_n > r'$$

i.e. $t_k - r'/3 < t_n < t_k + r'/3 \qquad s_k - r'/3 < s_n < s_k + r'/3 \qquad t_n - s_n > r'$

Now,

$$\begin{aligned}
(t_k + s_k)/2 - s_n &= \tfrac{1}{2}\,((t_k - s_n) + (s_k - s_n))\\
&> \tfrac{1}{2}\,((t_k - s_k - r'/3) - r'/3)\\
&> \tfrac{1}{2}\,(r' - r'/3 - r'/3)\\
&= r'/6\\
t_n - (t_k + s_k)/2 &= \tfrac{1}{2}\,((t_n - t_k) + (t_n - s_k))\\
&> \tfrac{1}{2}\,(-r'/3 + (t_k - r'/3 - s_k))\\
&> \tfrac{1}{2}\,(- r'/3 + (- r'/3 + r'))\\
&= r'/6
\end{aligned}$$

Let $r = (t_k + s_k)/2$. Then both $(r - s_n)$ and $(t_n - r)$ are positive sequence, i.e. $[r] \succ [(s_n)]$ and $[(t_n)] \succ [r]$. Hence $[(s_n)] \prec [r] \prec [(t_n)]$ for some $[r]\in\mathbb{R}_{\mathbb{Q}}$.

Q.E.D

The following theorem gives us a series of relationships between sequences in the old structure and the corresponding sequences in the new system.

Theorem:

Let $r_n, r\in\mathbb{Q}$. Then the following holds:

(i) $| [r] | = [| r |]$

(ii) $([r_n])$ is Cauchy iff (r_n) is Cauchy.

(iii) $([r_n]) \rightarrow [r]$ iff $(r_n) \rightarrow r$

(iv) $(r_n)\in[r]$ iff $([r_n]) \rightarrow [r]$

(v) Let $\alpha\in\mathbb{R}$ and $(r_n)\in\alpha$. Then $([r_n])$ is Cauchy and furthermore, $([r_n]) \rightarrow \alpha$.

(i) By isomorphism, $[r] \succ [0] \Rightarrow r > 0$, i.e. $| r | = r$

$[r] \prec [0] \Rightarrow r < 0$, i.e. $| r | = -r$

$[r] = [0] \Rightarrow r = 0$, i.e. $| r | = r$

Hence, $| [r] | = [r] = [| r |] \qquad \text{if } [r] \succcurlyeq [0]$

$-[r] = [-r] = [| r |] \quad \text{if } [r] \prec [0]$

i.e. $| [r] | = [| r |]$.

(ii) Suppose $([r_n])$ is Cauchy. Then given any rational $\varepsilon > 0$, $\exists\ k\in \mathbb{N}$ s.t $\forall\ n, m \geq k$, we have

$$| [r_n] \oplus (-[r_m]) | \prec [\varepsilon]$$
$$\Rightarrow | [r_n - r_m] | \prec [\varepsilon]$$
$$\Rightarrow [| r_n - r_m |] \prec [\varepsilon]$$
$$\Rightarrow | r_n - r_m | < \varepsilon \qquad \text{(by isomorphism)}$$

Hence (r_n) is also Cauchy.

Now suppose (r_n) is Cauchy. Given any real $\boldsymbol{\varepsilon} \succ [0]$, by denseness of rational, $\exists$ $[\varepsilon]\in \mathbb{R}_{\mathbb{Q}}$ s.t $[0] \prec [\varepsilon] \prec \boldsymbol{\varepsilon}$. Then $\exists\ k\in \mathbb{N}$ s.t $\forall\ n, m \geq k$,

$$| r_n - r_m | < \varepsilon$$
$$\Rightarrow [| r_n - r_m |] \prec [\varepsilon] \qquad \text{(by isomorphism)}$$
$$\Rightarrow | [r_n - r_m] | \prec [\varepsilon] \prec \boldsymbol{\varepsilon}$$
$$\Rightarrow | [r_n] \oplus (-[r_m]) | \prec \boldsymbol{\varepsilon}$$

Hence, $[r_n]$ is also Cauchy.

(iii) Suppose $[r_n]\rightarrow [r]$. Then for any rational $\varepsilon > 0$, $\exists\ k\in \mathbb{N}$ s.t $\forall\ n \geq k$, we have

$$| [r_n] \oplus (-[r]) | \prec [\varepsilon]$$
$$\Rightarrow [| r_n - r |] \prec [\varepsilon]$$
$$\Rightarrow | r_n - r | < \varepsilon \qquad \text{(by isomorphism)}$$

Hence $(r_n)\rightarrow r$.

Suppose $(r_n)\rightarrow r$. For any real $\boldsymbol{\varepsilon} \succ [0]$, by denseness of rational, $\exists$ $[\varepsilon]\in \mathbb{R}_{\mathbb{Q}}$ s.t $[0] \prec [\varepsilon] \prec \boldsymbol{\varepsilon}$. Then $\exists\ k\in \mathbb{N}$ s.t $\forall\ n \geq k$, we have

$$| r_n - r | < \varepsilon$$
$$\Rightarrow [| r_n - r |] \prec [\varepsilon] \prec \boldsymbol{\varepsilon}$$
$$\Rightarrow | [r_n] \oplus (-[r]) | \prec \boldsymbol{\varepsilon}$$

Hence, $([r_n])\rightarrow [r]$.

(iv) $(r_n)\in [r] \Leftrightarrow (r_n)\rightarrow r$

$$\Leftrightarrow ([r_n])\rightarrow [r] \quad \text{(by (iii))}$$

(v) Since (r_n) is Cauchy, (ii) tells us that $([r_n])$ is also Cauchy. Now, let any real $\boldsymbol{\varepsilon} \succ [0]$ be given. By denseness of rational, $\exists$ $[\varepsilon]\in \mathbb{R}_{\mathbb{Q}}$ s.t $[0] \prec [\varepsilon] \prec \boldsymbol{\varepsilon}$. Then $\exists\ k\in \mathbb{N}$ s.t $\forall\ n, m \geq k$, we have

$$| r_n - r_m | < \varepsilon/2$$
$$\Rightarrow -\varepsilon/2 < r_n - r_m < \varepsilon/2$$

Hence, for every fixed n s.t $n \geq k$, we have

$\varepsilon/2 < r_m - r_n + \varepsilon \qquad \forall\ m \geq k$

i.e. $(r_m - r_n + \varepsilon)$ is a positive sequence and so $[(r_m + \varepsilon)] \succ [r_n]$, i.e. $\alpha \oplus [\varepsilon] \succ [r_n]$

Also,

$r_n - r_m + \varepsilon > \varepsilon/2 \qquad \forall\ m \geq k$,

i.e. $(r_n - r_m + \varepsilon)$ is a positive sequence also and so $[(r_n + \varepsilon)] \succ [r_m]$, i.e. $[r_n] \oplus [\varepsilon] \succ \alpha$.

Hence, $\forall\ n \geq k$, we have

$[r_n] \oplus (-\alpha) \prec [\varepsilon] \qquad\qquad -[\varepsilon] \prec [r_n] \oplus (-\alpha)$

i.e. $| [r_n] \oplus (-\alpha) | \prec [\varepsilon] \prec \boldsymbol{\varepsilon}$

Hence, $([r_n])\rightarrow \alpha$.

Q.E.D

Let us now show that Cantor's approach really do give us a Cauchy Complete ordered field.

Theorem:

($\mathbb{R}$, $\oplus$, $\odot$, $\succ$) is Cauchy Complete.

Let (α_n) be any Cauchy sequence in $\mathbb{R}$. Now, by denseness of rational, for each $n\in\mathbb{N}$, $\exists\ [r_n]\in\mathbb{R}_{\mathbb{Q}}$ s.t

$\alpha_n \oplus (-[1/n]) \prec [r_n] \prec \alpha_n \oplus [1/n]$, i.e. $|\,[r_n] \oplus (-\alpha_n)\,| \prec [1/n]$.

Let any real $\boldsymbol{\varepsilon} \succ [0]$ be given. Since (α_n) is Cauchy, $\exists\ k_1\in\mathbb{N}$ s.t

$|\,\alpha_n \oplus (-\alpha_m)\,| \prec \boldsymbol{\varepsilon}/3 \qquad \forall\ n\geq k.$

By denseness of rational, $\exists\ [\varepsilon]\in\mathbb{R}_{\mathbb{Q}}$ s.t $[0] \prec [\varepsilon] \prec \boldsymbol{\varepsilon}/3$. By Archimedean property for $\mathbb{Q}$, $\exists\ k_2\in\mathbb{N}$ s.t

$1/k_2 < \varepsilon$, hence $1/n < \varepsilon\ \forall\ n \geq k_2$. By isomorphism, we can then claim

$[1/n] \prec [\varepsilon] \prec \boldsymbol{\varepsilon}/3\ \forall\ n \geq k_2$

Take $k = \max(k_1, k_2)$. Then

$$\begin{aligned}
|\,[r_n] \oplus (-[r_m])\,| &= |\,([r_n] \oplus (-\alpha_n)) \oplus (\alpha_n \oplus (-\alpha_m)) \oplus (\alpha_m \oplus (-[r_m]))\,| \\
&\preccurlyeq |\,[r_n] \oplus (-\alpha_n)| \oplus |\,\alpha_n \oplus (-\alpha_m)\,| \oplus |\,\alpha_m \oplus (-[r_m])\,| \\
&\prec [1/n] \oplus |\,\alpha_n \oplus (-\alpha_m)\,| \oplus [1/m] \\
&\prec \boldsymbol{\varepsilon}/3 \oplus \boldsymbol{\varepsilon}/3 \oplus \boldsymbol{\varepsilon}/3 && \forall\ n, m \geq k \\
&= \boldsymbol{\varepsilon} && \forall\ n, m \geq k
\end{aligned}$$

This means $([r_n])$ is also a Cauchy sequence. Hence (r_n) is also a Cauchy sequence in $\mathbb{Q}$. Hence $\alpha = [(r_n)]$ will be in $\mathbb{R}$. Hence, we will have $([r_n]) \to \alpha$. Now. let any real $\boldsymbol{\varepsilon} \succ [0]$ be given. Then $\exists\ k_1\in\mathbb{N}$ s.t

$|\,[r_n] \oplus (-\alpha)\,| \prec \boldsymbol{\varepsilon}/2 \qquad \forall\ n \geq k_1.$

Similar to above, by denseness of rational and Archimedean property for $\mathbb{Q}$, $\exists\ k_2\in\mathbb{N}$ s.t

$[1/n] \prec \boldsymbol{\varepsilon}/2 \qquad \forall\ n \geq k_2.$

Hence, take $k = \max(k_1, k_2)$ and we have

$$\begin{aligned}
|\,\alpha_n \oplus (-\alpha)\,| &= |\,(\alpha_n \oplus (-[r_n])) \oplus ([r_n] \oplus (-\alpha))\,| \\
&\preccurlyeq |\,\alpha_n \oplus (-[r_n])\,| \oplus |\,[r_n] \oplus (-\alpha)\,| \\
&\prec [1/n] \oplus |\,[r_n] \oplus (-\alpha)\,| \\
&\prec \boldsymbol{\varepsilon}/2 \oplus \boldsymbol{\varepsilon}/2 && \forall\ n \geq k \\
&= \boldsymbol{\varepsilon} && \forall\ n \geq k
\end{aligned}$$

Hence, $(\alpha_n) \to \alpha$.

Hence, ($\mathbb{R}$, $\oplus$, $\odot$, $\succ$) is Cauchy Complete.

Q.E.D

Our new system also has the Archimedean Property as shown below. Let us first make a small definition to state techinically what $\mathbb{R}_{\mathbb{N}}$ means.

Defn: We define $\mathbb{R}_{\mathbb{N}}$ to be

$\mathbb{R}_{\mathbb{N}} = \{[n] \in \mathbb{R}_{\mathbb{Q}} | n \in \mathbb{N}\}$

Theorem: Archimedean Property

For every $[(r_n)], [(s_n)] \in \mathbb{R}$ s.t $[(r_n)] \succ [0]$, $\exists [n] \in \mathbb{R}_{\mathbb{N}}$ s.t $[n] \odot [(r_n)] \succ [(s_n)]$.

If $[(r_n)] \succ [(s_n)]$, then since $[1] \in \mathbb{R}_{\mathbb{N}}$, there is nothing to prove. Hence, we can assume $[(s_n)] \succcurlyeq [(r_n)] \succ [0]$. By denseness of rational, $\exists$ $[r]$, $[s] \in \mathbb{R}_{\mathbb{Q}}$ s.t $[(s_n)] \oplus [1] \succ [s] \succ [(s_n)] \succcurlyeq [(r_n)] \succ [r] \succ [0]$.

Under isomorphism, we invoke the Archimedean property of $\mathbb{Q}$ so $\exists$ $[n] \in \mathbb{R}_{\mathbb{N}}$ s.t $[n] \odot [r] \succ [s]$. We then have

$[n] \odot [(r_n)] \succ [n] \odot [r] \succ [s] \succ [(s_n)]$

i.e. $[n] \odot [(r_n)] \succ [(s_n)]$

Hence, the Archimedean property holds.

Q.E.D

Let us now define formally what a Cantor Real Number System really is.

Defn: For any ordered field ($\mathbb{R}_C$, $\oplus$, $\odot$, $\succ$), we say that it is a Cantor Real Number System if

(i) $\exists$ a subfield ($\mathbb{Q}_C$, $\oplus$, $\odot$, $\succ$) that is isomorphic to ($\mathbb{Q}$, +, ., >).

(ii) ($\mathbb{R}_C$, $\oplus$, $\odot$, $\succ$) is Cauchy Complete

(iii) ($\mathbb{R}_C$, $\oplus$, $\odot$, $\succ$) has the Archimedean property.

Hence, our new system is actually a Cantor Real Number System and so Cantor Real Number System does exist. From now on, we shall henceforth speak only of a general Cantor real number system denoted by ($\mathbb{R}$, +,. ,>). The various important subsets of natural numbers, integers and rationals will be naturally denoted by $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ respectively. Since the Dedekind real number system is Cauchy complete and has the Archimedean property, we can see that the Dedekind Real Number system is actually a Cantor Real Number System. The following theorem tells us that the converse is also true.

Theorem:

($\mathbb{R}$, +, ., >) is order complete.

Take any non-empty subset of A of $\mathbb{R}$ that is bounded above by some u_0. Let $U = \{u \in \mathbb{R} \mid u$ is an upper bound of A$\}$. Since $A \neq \phi$, $\exists$ $a_0 \in A$. By Archimedean property, $\exists$ $m \in \mathbb{N}$ s.t $m > -a_0$, i.e. $a_0 < -m$ so $-m \notin U$. We define 2 sequences (x_n), (y_n) as such:

$x_1 = -m$ ($\notin U$)

$y_1 = u_0$ ($\in U$)

Suppose that $x_n \notin U$ and $y_n \in U$. Define

$x_{n+1} = \frac{1}{2}(x_n + y_n)$ if $\frac{1}{2}(x_n + y_n) \notin U$

x_n otherwise

$y_{n+1} = \frac{1}{2}(x_n + y_n)$ if $\frac{1}{2}(x_n + y_n) \in U$
$\quad y_n$ otherwise

By definition, note that we then have $x_n \notin U$, $y_n \in U$ $\forall$ $n \in \mathbb{N}$.

Hence, for every n, $\exists$ $a_n \in A$ s.t $x_n < a_n \leq y_n$, i.e. $x_n < y_n$.

Let $N = y_1 - x_1 > 0$. We first make a few observations.

If $\frac{1}{2}(x_n + y_n) \in S$, then $y_{n+1} - x_{n+1} = \frac{1}{2}(x_n + y_n) - x_n = \frac{1}{2}(y_n - x_n)$

If $\frac{1}{2}(x_n + y_n) \notin S$, then $y_{n+1} - x_{n+1} = y_n - \frac{1}{2}(x_n + y_n) = \frac{1}{2}(y_n - x_n)$

Hence $y_{n+1} - x_{n+1} = \frac{1}{2}(x_n + y_n)$ $\forall$ $n \in \mathbb{N}$.

Hence
$$\begin{aligned} y_n - x_n &= \tfrac{1}{2}(x_{n-1} + y_{n-1}) \\ &= \tfrac{1}{2}(\tfrac{1}{2}(x_{n-2} + y_{n-2})) \\ &\vdots \\ &= N/2^{n-1} \ \forall\ n \in \mathbb{N}. \end{aligned}$$

For every $n \in \mathbb{N}$, either $y_n = y_{n+1}$ or
$$\begin{aligned} y_n - y_{n+1} &= y_n - \tfrac{1}{2}(x_n + y_n) \\ &= \tfrac{1}{2}(y_n - x_n) \\ &= N/2^n \\ &> 0 \end{aligned}$$
i.e. $y_{n+1} \leq y_n$ and so (y_n) is decreasing.

For every $n \in \mathbb{N}$, either $x_n = x_{n+1}$ or
$$\begin{aligned} x_{n+1} - x_n &= \tfrac{1}{2}(x_n + y_n) - x_n \\ &= \tfrac{1}{2}(y_n - x_n) \\ &= N/2^n \\ &> 0 \end{aligned}$$
i.e. $x_{n+1} \geq x_n$ and so (x_n) is increasing.

If $m, n \in \mathbb{N}$ are s.t $m < n$, we have
$$\begin{aligned} 0 < y_m - y_n &< y_m - x_n \ (\because\ y_n > x_n) \\ &< y_m - x_m \ (\because\ x_n > x_m) \\ &= N/2^{m-1} \end{aligned}$$
i.e. $|\, y_m - y_n \,| < N/2^{m-1}$

Let any $\varepsilon > 0$ be given.

By Archimedean property, $\exists$ $k' \in \mathbb{N}$ s.t
$N < k'\varepsilon$

By the exponentiation version of Archimedean property for $\mathbb{N}$, $\exists$ $k \in \mathbb{N}$ s.t
$2^k > k'$

Hence, $\forall$ $n \geq k$, we have
$2^n \geq 2^k > k'$
i.e. $\varepsilon 2^n \geq \varepsilon 2^k > \varepsilon k' > N$, i.e. $N/2^n < \varepsilon$

Hence,
$|\, y_m - y_n \,| < N/2^{m-1}$ (by symmetry of absolute order, we can always assume $m < n$. If $m = n$, then trivially we have $|\, y_m - y_n \,| = 0 < N/2^{m-1}$)
$\quad < \varepsilon \quad \forall$ $n, m \geq k + 1$

Hence, we have shown that (y_n) is Cauchy. By Cauchy Completeness, (y_n) converges to some $y \in \mathbb{R}$.

Suppose $y \notin U$. Then $\exists\ a \in A$ s.t $a > y$. By density theorem, $\exists\ z \in \mathbb{R}$ s.t $a - y > z > 0$. Since we always have $y_n \geq a$, we will have $y_n - y \geq a - y > z > 0$. But $(y_n) \rightarrow y$, i.e. for $\varepsilon = z/2$, $\exists\ k \in \mathbb{N}$ s.t

$| y_n - y | < z/2 \quad \forall\ n \geq k$

In particular,

$y_k - y \leq | y_n - y | < z/2 < z < y_k - y$, a contradiction!

Hence, $y \in U$.

Now suppose $\exists\ u \in U$ s.t $u < y$. Note first that similar to above, by Archimedean property and its exponentiation version for $\mathbb{N}$, given any $\varepsilon > 0$, $\exists\ k \in \mathbb{N}$ s.t

$N/2^n < \varepsilon \quad \forall\ n \geq k$

i.e. $| (y_n - x_n) - 0 | = y_n - x_n$ ($\because\ y_n - x_n > 0$)

$= N/2^{n-1}$

$< \varepsilon \quad \forall\ n \geq k + 1$

i.e. $(y_n - x_n) \rightarrow 0$

Now, if $\exists\ y_k$ s.t $y_k < y$, then we have $y_n \leq y_k < y \ \ \forall\ n \geq k$ as (y_n) is decreasing. But $(y_n) \rightarrow y$ so for $\varepsilon = y - y_k > 0$, $\exists\ N \in \mathbb{N}$ s.t

$| y_n - y | < y - y_k \quad \forall\ n \geq \mathbb{N}$

For $N' = \max(k, N)$, we have in particular

$| y_{N'} - y | = -(y_{N'} - y) \qquad | y_{N'} - y | < y - y_k$

$\Rightarrow -(y_{N'} - y) < y - y_k$

$\Rightarrow y_{N'} > y_k$, contradicting (y_n) being decreasing!

Hence, we always have $y_n - y \geq 0$.

Since $(y_n - x_n) \rightarrow 0$, for $\varepsilon = y - u > 0$, $\exists\ k \in \mathbb{N}$ s.t

$y_n - x_n = | y_n - x_n | < y - u$, i.e. $y_n - y < x_n - u \quad \forall\ n \geq k$

In particular,

$0 \leq y_k - y < x_k - u$, i.e. $x_k > u$.

But this means $x_k > u \geq a\ \forall\ a \in A$, making x_k an upper bound, which is a contradiction! Hence, $y \leq u\ \forall\ u \in U$ and so $\text{Sup}A = y$ exists.

Since $(\mathbb{R}, +, ., >)$ has the least upper bound property, it is hence order complete.

Q.E.D

Hence, a Cantor Real Number system is also the Dedekind Real number system. This means that there is no point pursuing the properties of the Cantor Real number system(note that it is unique since Dedekind Real number system is unique) since those desired properties has already been shown in Chapter 4.1! Hence, let us end this chapter and proceed on to the final conclusion.

End Of Chapter 4.2

Conclusion

We have mentioned eariler that it is quite difficult for the intuition to conceive of an irrational number. Hence, in creating the real number system, we have not laid down in a tablet of stone the exact conditions that the real number system must have. Rather, we pretend that we do not know exactly what the real number system should be, and we went on to pursue the intuition of Richard Dedekind and Georg Cantor. Both gives us an approach that sound reasonable but we are not exactly sure. Eventually, we realise, after a wild goose chase, that these two approaches actually converge to the same unique number system. Indeed, great minds think alike. But the stubborn question still remains: Is that our familar real number system?

On the intuitive side, this question should receive a resounding yes. The rationals is to us quite a natural thing, and if we do not discover by abstraction that there are actually 'holes', we would never have bothered to invent a system of real numbers at all. Hence, we do not have to worry whether we have managed to fill in enough holes to make it *the real number system*. Instead, the real number system should be any system that is produced by our natural process of gap-filling. That is to say, we do not question whether Dedekind did manage to achieve the real number system. After all, we ourselves do not even know what the real number system is. The important thing is that Dedekind did manage to construct from the rationals a system that is not only consistent with the normal operation of the rationals but also free from the problem of the unmeasurable triangle. So it is as good a real number system to us as any ideal absolute one that some might believe exist out there somewhere. The fact that Cantor, with another natural approach, ended up with the same system should give us more conviction on this view. Nonetheless, what an abstract object is supposed to be can be something very difficult to argue about. If one feels very strongly that the real number system must have some strange properties that is absent in our Dedekind real number system, then after centuries of debate, the author believes that we will still be standing on square one.

Hence, let us look instead at the technical side and see whether we have constructed a system that mathematicians can easily substitute for their assumed real number system. In most mathematical textbooks that have needs to refer to the real number system, they usually give a list of properties that they assumed the real number system to have. In most cases, the properties reduce to nothing more than saying that the real number system is a complete ordered field, which is hence our Dedekind real number system. Of course, we do require the existence of a substructure that is a model of the rationals, but it is easy to show that any infinite field contain a copy of the rationals so this does not really bother us. For a concrete example, the author refer the reader to the text **Introduction to Real Analysis 2$^{\text{nd}}$ Edition**, by Robert G. Bartle and Donald R. Sherbert. The text assume 3 major properties of $\mathbb{R}$:

a) Algebraic properties(Chapter 2, Section 2.1, pg 23)

This just mean that $\mathbb{R}$ is a field.

b) Order properties (Chapter 2, Section 2.2, pg 29)

This just assume that the field is ordered

c) The Completeness property (Chapter 2, Section 2.4, pg 42)

This just assume that the ordered field is in fact order complete.

Most mathematical undergraduates in the National University of Singapore should be familar with this text. It is the text commonly employed as a reference in MA2108, introduction to real analysis. Hence, we have indeed created the real number system, or at least *that* real number system assumed for most of mathematical analysis.

Assuming that we are talking about the real number system that mathematicians have been using, our project in fact allows us to say two fundamental things about the system. Firstly, **the real number system is unique and any complete ordered field is in fact the real number system**. Secondly, **an ordered field is Cauchy complete and possesses the Achimedean property if and only if it is order complete**. This should provide us with two alternatives whenever we wish to check whether a given system is the real number system. These two statements are not exactly trivial, and so we will let them serve as the concluding statements of this project.

In all, it is hoped that through this construction, one would gain a better insight on how our number system actually works. Also, we can see better the relationship between the fundamental subsets such as the integer and the natural numbers. Before we terminate this chapter, let us not forget about Peano, the person that provide us with the divine axioms. **Peano's axioms allows us to create one and only one natural number system, integer system, field of rational, and finally the real number system!** This indicate to us that an alien civilization possessing just *the similar innate ability to count* and the same logic function should come up with the same number system. But we are digressing again...What the author really want to say is...the end! Thank you!

End Of Chapter 4

Reference

From Numbers To Analysis	*Inder K.Rana*
Introduction To Real Analysis 2nd Edition	*Robert G.Bartle, Donald R. Sherbert*