5-1964

A Development of the Number System

Janet R. Olsen
Utah State University

A DEVELOPMENT OF THE NUMBER SYSTEM

by

Janet R. Olsen

A thesis submitted in partial fulfillment
of the requirements for the degree

of

MASTER OF SCIENCE

in

Mathematics

Approved:

UTAH STATE UNIVERSITY
Logan, Utah

1964

ACKNOWLEDGMENT

I wish to express my sincere gratitude to Dr. Neville C. Hunsaker for his help and guidance in the preparation of this thesis.

TABLE OF CONTENTS

INTRODUCTION

This paper is based on Landau's book "Foundations of Analysis" which constitutes a development of the number system founded on the Peano axioms for natural numbers.

In order to show mastery of the subject matter this paper gives a somewhat different organization of material and modified or more detailed proofs of theorems. In situations where proofs become rather routine repetitions of previously noted techniques the proofs are omitted.

The following symbols and notation are used. Natural numbers are denoted by lower case letters such as a,b,c,...x,y,z. Sets are denoted by upper case letters such as M, N, ...X, Y, Z. If a is an element of M, this will be written $a \in M$. The denial of this is written $a \notin M$. The symbol $\exists/x$ is read "There exists an unique x". If x and y are names for the same number we write $x=y$. It is assumed that the relation $=$ is an equivalence relation; i.e., (1) $x=x$, (2) if $x=y$, then $y=x$, (3) if $x=y$ and $y=z$, then $x=z$. Throughout this paper there will be no special attempt to distinguish between the name of a number and the number itself. For example, the phrase " if x is a number" will be used in place of " if x is the name of a number."

NATURAL NUMBERS

Definition 1.1. A set N of elements is called the natural numbers if and only if the following axioms are satisfied:

Axiom 1.I. For each $x \in N$, there exists an unique element of N called the successor of x, denoted by x'; i.e., if $x=y$ then $x'=y'$.

Axiom 2.I. There exists an element of N, denoted by 1, such that $x' \neq 1$ for every $x \in N$.

Axiom 3.I. If $x'=y'$, then $x=y$.

Axiom 4.I. If a set M of natural numbers contains the element 1 and it contains x' whenever it contains x, then M is the same set as N.

Addition and Multiplication

In this section two binary operations called addition and multiplication are defined on the natural numbers. It is shown that these operations obey the commutative and associative laws; also, that multiplication is distributive with respect to addition. One main result of the definition of addition will be that either two natural numbers, x and y, are the same natural number; or, there exists uniquely a natural number u such that $x=y+u$; or, there exists uniquely a natural number v such that $y=x+v$.

Theorem 1.2. If $x \neq 1$, $\exists/u$ such that $x=u'$.

Proof. The uniqueness of u is easily established. Suppose there exist u and v such that $x=u'$ and $x=v'$. Then $u'=v'$ which implies $v=u$ by Axiom 3. To show there exists such an u let $M = \{x : x \in N$ and if $x \neq 1$, there exists $u \in N$ such that $u'=x\} \cup \{1\}$. We note that

$1 \in N$ by Axiom 2 and that $1 \in M$ by the construction of set M. And to see that $x' \in M$ whenever $x \in M$ we note that $x' \in N$ by Axiom 1 and so there exists an $u \in N$ such that $u'=x'$; namely, $x'=x'$. Therefore, by Axiom 4, M is the same set as N.

Theorem 1.3. There exists an unique binary operation to be called addition, denoted by +, which assigns to each ordered pair of natural numbers (x,y) a natural number, to be denoted by x=y, such that for every x and y:

i) $x+1=x'$

and ii) $x+y'=(x+y)'$.

Proof. The uniqueness of the operation will be established first. Suppose there exists two operations denoted by + and * such that:

iii) $x+1=x'$, and $x+y'=(x+y)'$

and iv) $x*1=x'$, and $x*y'=(x*y)'$.

Let x be given and let $M = \{y: x+y=x*y\}$. Now $1 \in M$ since $x+1=x'=x*1$ by (iii) and (iv). If $y \in M$, $y' \in M$ since

$$\begin{aligned} x+y' &= (x+y)' \text{ by (iii)} \\ &= (x*y)' \text{ because } y \in M \\ &= x*y' \text{ by (iv).} \end{aligned}$$

Therefore $x+y'=x*y'$ and M is the same set as N by Axiom 4. Hence $x+y=x*y$ for every x and y; that is, if the binary operation exists, it is unique.

Now it will be shown that such an operation exists which satisfies (i) and (ii). Let y be given and let $M = \{x:$ for the ordered pair (x,y) such an $x+y$ exists$\}$. For $x=1$, define (v) $1+y=y'$. If $y \in N$, y' exists and $y' \in N$ by Axiom 1. Thus $1+y$ exists and is an element of N. We need to show that for $x=1$, $x+1=x'$ and $x+y'=(x+y)'$.

For the first: $x+1 = 1+1$ since $x=1$

$= 1'$ by (v)

$= x'$ by Axiom 1 since $x=1$.

As to the latter: $x+y' = 1+y'$ since $x=1$

$= (y')'$ by (v)

$= (1+y)'$ by (v)

$= (x+y)'$ since $x=1$.

Thus, $1 \in M$.

If $x \in M$, there exists an $x+y$ for the ordered pair (x,y) which satisfies (i) and (ii). For x', define (vi) $x'+y = (x+y)'$. Again (i) and (ii) must be satisfied with this definition for x'; i.e., $x'+1 = (x')'$ and $x'+y' = (x'+y)'$.

For the first: $x'+1 = (x+1)'$ by (vi)

$= (x')'$ by (i) since $x \in M$.

As to the second: $x'+y' = (x+y')'$ by (vi)

$= ((x+y)')'$ by (ii) since $x \in M$

$= (x'+y)'$ by (vi)

Hence, $x'+y' = (x'+y)'$. Therefore, $1 \in M$ and $x' \in M$ whenever $x \in M$. Thus, M is the same set as N by Axiom 4. The existence of the unique binary operation addition which assigns to each ordered pair of natural numbers (x,y) the natural number named $x+y$ satisfying:

a) $x+1 = x' = 1+x$

and b) $x+y' = (x+y)' = x'+y$

has been established.

Theorem 1.4. (Associative Law of Addition). For every $x,y,z \in N$ $(x+y) + z = x + (y+z)$.

Proof. Let x and y be given, and let $M = \{z: (x+y)+z = x+(y+z)\}$.

Now $1 \in M$ since

$$(x+y) + 1 = (x+y)' \text{ by 1.3 (i)}$$
$$= x+y' \text{ by 1.3 (ii)}$$
$$= x+(y+1) \text{ by 1.3 (i).}$$

and thus $(x+y) + 1 = x+(y+1)$. If $z \in M$, $z' \in M$ since

$$(x+y) + z' = \big((x+y) + z\big)' \text{ by 1.3 (ii)}$$
$$= \big(x + (y+z)\big)' \text{ because } z \in M$$
$$= x + (y+z)' \text{ by 1.3 (ii)}$$
$$= x + (y+z') \text{ by 1.3 (ii)}$$

and thus $(x+y) + z' = x + (y+z')$. Therefore, M is the same set as N and the proof of this theorem is complete.

Theorem 1.5. (Commutative Law of Addition). For every $x,y \in N$, $x+y = y+x$.

Proof. Let x be given, and let $M = \{y\colon x+y = y+x\}$. For $y=1$, $x+1 = x' = 1+x$ by 1.3 (i) and (v). Hence, $1 \in M$.

If $y \in M$, $y' \in M$ since $x+y' = (x+y)'$ by 1.3 (ii)

$$= (y+x)' \text{ since } y \in M$$
$$= y'+x \text{ by 1.3 (vi)}$$

and thus $x+y' = y'+x$. Therefore, M is the same set as N.

Theorem 1.6. Given x and y, one and only one of the following must occur: i) $x=y$

or ii) There exists an unique u such that $x=y+u$

or iii) There exists an unique v such that $x+v=y$.

Proof. (The proof of this theorem involves the following theorems whose proofs we do not include since they are rather straightforward applications of the axiom of induction: a) $y \neq y+u$ for all $u \in N$

b) if $y \neq z$, then $x+y \neq x+z$)

First, it will be shown that the three cases are incompatible. If (i) and (ii) both occur then $x=y$ and $x=y+u$ imply $y=y+u$ which is impossible since $y \neq y+u$ for all u by a). Similarly, (i) and (iii) are incompatible. For (ii) and (iii), $x=y+u$ and $x+v=y$ imply $y=(y+u)+v=y+(u+v)$ by 1.4. Therefore, $y=y+(u+v)$ which is impossible since $y \neq y+u$ for all u. Hence, only one of the three cases occurs.

Next, it will be shown that the u in (ii) is unique. Assume there exist two natural numbers, u and t, such that $x=y+u$ and $x=y+t$. Hence $y+u=y+t$ which implies $u=t$; since if $u \neq t$, $y+u \neq y+t$ by b). Thus, the u is unique. Similarly, the v in (iii) can be shown to be unique.

Last, it will be shown that one of the three cases must occur. Let x be given and let $M=\{y:$ one of the three cases occurs$\}$. If $y=1$; either $x=1$ and $x=y$ [Case (i) for 1], or $x \neq 1$ and $x=u'$ by 1.2. If $x=u'=1+u$ by 1.3(v), then $x=y+u$ since $y=1$ [Case (ii) for 1]. Therefore, $1 \in M$. If $y \in M$, one of the three cases must occur. Case (i) for y, $y=x$. Thus, $y'=x'=x+1$ [Case (iii) for y']. Case (ii) for y, $x=y+u$. If $u=1$, then $x=y+1=y'$ [Case (i) for y']. If $u \neq 1$, $u=w'$ by 1.2. If $u=w'$ then

$$\begin{aligned} x &= y+w' \\ &= y+(1+w) \text{ by } 1.3(v) \\ &= (y+1)+w \text{ by } 1.4 \\ &= y'+w \text{ by } 1.3(i) \end{aligned}$$

Thus, $x=y'+x$ [Case (ii) for y']. Case (iii) for y, $y=x+v$.

$$\begin{aligned} \text{Hence } y' &= (x+v)' \\ &= x+v' \text{ by } 1.3\text{ (ii)} \end{aligned}$$

[Case (iii) for y']. In any case $y' \in M$ whenever $y \in M$. Thus, M is the same set as N and the theorem is established.

Theorem 1.7. There exists an unique binary operation, to be called multiplication, denoted by $\cdot$, which assigns to each ordered pair of natural numbers (x,y) a natural number, to be denoted by $x \cdot y$, such that for every x and y: i) $x \cdot 1 = x$

and ii) $x \cdot y' = x \cdot y + x$.

Proof. The uniqueness of the operation will be established first. Suppose there exist two operations, denoted by $\cdot$ and $*$ such that:

iii) $x \cdot 1 = x$ and $x \cdot y' = x \cdot y + x$

and iv) $x * 1 = x$ and $x * y' = x * y + x$.

Let x be given and let $M = \{y : x \cdot y = x * y\}$. Now, $1 \in M$ since $x \cdot 1 = x = x * 1$ by (iii) and (iv). If $y \in M$, $y' \in M$ since

$x \cdot y' = x \cdot y + x$ by (iii)

$= x * y + x$ since $y \in M$

$= x * y'$ by (iv)

Therefore $x \cdot y' = x * y'$ and M is the same set as N. Thus, the binary operation is unique, if it exists.

Now to show that it is possible to define a binary operation so that for every x and y; $x \cdot 1 = x$ and $x \cdot y' = x \cdot y + x$. Let y be given and let $M = \{x$: for the ordered pair (x,y) such an $x \cdot y$ exists$\}$.

For $x=1$, define (v) $1 \cdot y = y$. We need to show that $x \cdot 1 = x$ and $x \cdot y' = x \cdot y + x$. Now $x \cdot 1 = 1 \cdot 1$ since $x=1$

$= 1$ by (v)

$= x$ since $x=1$.

Thus the first condition is satisfied.

As for the second: $x \cdot y' = 1.y'$ since $x=1$

$= y'$ by (v)

$= y+1$ by 1.3 (i)

$= 1\cdot y+1$ by (v)

$= x\cdot y+x$ since $x=1$

Hence, if $x=1$, $x\cdot y' = xy+x$. Thus, $1 \in M$.

If $x \in M$, there exists an $x\cdot y$ for each ordered pair (x,y) which satisfies (i) and (ii). For x', define vi) $x'\cdot y = x\cdot y+y$. Again conditions (i) and (ii) are satisfied for: if $y=1$ then

$x'\cdot 1 = x\cdot 1 + 1$ by (v)

$= x+1$ by (i) since $x \in M$

$= x'$ by 1.3 (i)

Thus, $x'\cdot 1 = x'$.

Now, $x'\cdot y' = x\cdot y' + y'$ by (vi)

$= (x\cdot y+x) + y'$ by (ii) since $x \in M$

$= x\cdot y + (x+y')$ by 1.4

$= x\cdot y + (x+y)'$ by 1.3 (ii)

$= x\cdot y + (x'+y)$ by 1.3 (vi)

$= x\cdot y + (y+x')$ by 1.5

$= (x\cdot y+y) + x'$ by 1.4

$= x'y + x'$ by (vi).

Therefore, $x'\cdot y' = x'\cdot y + x'$. Hence, $1 \in M$ and $y' \in M$ if $y \in M$. Thus, M is the same set as N and the binary operation multiplication which assigns to each ordered pair of natural numbers (x,y) the natural number named $x\cdot y$ such that a) $x\cdot 1 = x = 1\cdot x$

and b) $x\cdot y' = x\cdot y + x$

and c) $x'\cdot y = x\cdot y + y$

exists and is unique.

Hereafter, the sign of multiplication will be omitted. Thus, $x \cdot y$ will be written xy.

Theorem 1.8. (Commutative Law of Multiplication). For every $x, y \in N$, $xy = yx$.

Proof. The proof of this theorem is similar to the proof of theorem 1.5 and will be omitted.

Theorem 1.9. (Distributive Law). For every $x, y, z \in N$, $x(y+z) = xy + xz$.

Proof. Let x and y be given, and let $M = \{z : x(y+z) = xy + xz\}$.

Now, $1 \in M$ since $x(y+1) = xy'$ by 1.3 (i)

$= xy + x$ by 1.7 (ii)

$= xy + x \cdot 1$ by 1.3 (i).

and so $x(y+1) = xy + x \cdot 1$. If $z \in M$, $z' \in M$

since $x(y+z') = x(y+z)'$ by 1.3 (ii)

$= x(y+z) + x$ by 1.7 (ii)

$= (xy + xz) + x$ since $z \in M$

$= xy + (xz + x)$ by 1.4

$= xy + xz'$ by 1.7 (ii)

and thus $x(y+z') = xy + xz'$. Therefore, M is the same set as N and the theorem is shown.

Theorem 1.10. (Associative Law of Multiplication) For every $x, y, z \in N$, $(xy)z = x(yz)$.

Proof. Let x and y be given, and let $M = \{z : (xy)z = x(yz)\}$.

Now, $1 \in M$ since $(xy) \cdot 1 = xy$ by 1.7 (i)

$= x(y \cdot 1)$ by 1.7 (i)

If $z \in M$, $z' \in M$ since $(xy)z' = (xy)z + xy$ by 1.7 (ii)

$= x(yz) + xy$ since $z \in M$

$= x\ (yz+y)$ by 1.9

$= x\ (yz')$ by 1.7 (ii).

Thus, $(xy)z' = x(yz')$ and M is the same set as N.

Ordering

In this section the basic definitions of greater than and less than are given. The main result to be established is that every nonempty set of natural numbers contains a least one.

Definition 1.11. $x > y$ if and only if there exists a natural number u such that $x = y+u$.

Definition 1.12. $x < y$ if and only if $y > x$.

Theorem 1.13. Let x and y be given, then one and only one of the following occur: $x=y$ or $x > y$ or $x < y$.

Proof. The proof follows directly from 1.6, 1.11 and 1.12.

Definition 1.14. $x \geq y$ if and only if $x=y$ or $x > y$.

Definition 1.15. $x \leq y$ if and only if $y \geq x$.

Theorem 1.16. If $x < y$ and $y < z$, then $x < z$.

Proof. Trivial

Theorem. 1.17. For all $x \in N$, $x+y > x$.

Proof. Now, $x+y = x+y$. Therefore, $x+y > x$ by 1.11.

Theorem 1.18. $x=y$ or $x > y$ or $x < y$ if and only if $x+z = y+z$ or $x+z > y+z$ or $x+z < y+z$, respectively.

Proof. Suppose $x=y$. Then obviously $x+z = y+z$. If $x > y$ then there exists u such that $x=y+u$. Hence,

$x + z = (y+u) + z$ by first part.

$= y + (u+z)$ by 1.4

$= y + (z+u)$ by 1.5

$= (y+z) + u$ by 1.4.

Therefore, $x+z > y+z$ by 1.11. If $x < y$ then $y > x$ by 1.12. Hence by above part $y+z > x+z$ and by 1.12, $x+z < y+z$.

The converse follows immediately from the preceding proof, and the fact that the three cases are mutually exclusive and exhaust all possibilities.

Theorem 1.19. $x=y$ or $x > y$ or $x < y$ if and only if $xz = yz$ or $xz > yz$ or $xz < yz$, respectively.

Proof. Suppose $x=y$. Then obviously $xz = yz$. If $x > y$ there exists u such that $x=y+u$. Thus, $xz = (y+u)z$ by first part

$= z(y+u)$ by 1.8

$= zy + zu$ by 1.9

$= yz + zu$ by 1.8.

Hence, $xz > yz$ by 1.11. If $x < y$ then $y > x$ and by preceding part $yz > xz$ which implies $xz < yz$ by 1.12.

The converse follows immediately from the preceding proof and the fact that the three cases are mutually exclusive and exhaust all possibilities.

Theorem 1.20. For all $x,y \in N$ if $y > x$ then $y \geq x+1$.

Proof. Since $y > x$ there exists u such that $y = x+u$. Either $u=1$, hence $y=x+1$; or $u \neq 1$ and so $u=w'$ by 1.2. Hence,

$x+u = x+w'$ by 1.18

$= x + (1+w)$ by 1.3 (v)

$= (x+1) + w$ by 1.4.

Thus, $y > x+1$ by 1.11. In either case if $y > x$ then $y \geq x+1$ by 1.14.

Theorem 1.21. For every $x \in N$, $x \geq 1$.

Proof. Either $x=1$ or $x \neq 1$ in which case $x=u'$ by 1.2. Therefore if $x=u' = 1+u$ by 1.3(v), $x > 1$ by 1.11. Hence, $x \geq 1$ by 1.14.

Theorem 1.22. In every nonempty set T of natural numbers, there is one which is less than every other element of the set. That is, there exists an $x \in T$ such that $x \leq y$ for all $y \in T$.

Proof. Let M be the set of all z such that $z \in N$ and $z \leq y$ for all $y \in T$. M is not empty because $1 \in M$ by 1.21. M does not contain all natural numbers since for any $y \in T$ $y+1 > y$ by 1.17 and thus $y+1 \notin M$. There exists an element of M, denote it by x, such that $x+1 \notin M$. For if $x+1 \in M$ whenever $x \in M$, M would be the same set as N by Axiom 4 since $1 \in M$. This contradicts the fact that M does not contain all the natural numbers. Since $x \in M$, $x \leq y$ for all $y \in T$. Now, x is also an element of T. To show this assume $x \notin T$. Then $x < y$ for all $y \in T$. Therefore $x+1 \leq y$ for all $y \in T$ by 1.20. Thus, $x+1 \in M$ which contradicts the fact that $x+1 \notin M$. Hence, $x \in T$ and is less than every other element of the set.

RATIONAL NUMBERS

Two new types of numbers are defined in this section. The first, the fraction, is defined in terms of natural numbers; and the second, the rational number, is defined in terms of fractions. The binary operations of addition and multiplication on the rational numbers are defined, then the associative, commutative, and distributive properties are established; as well as the facts that there is no greatest or least rational number, and given any two distinct rational numbers there is at least one rational number which is less than one of the given rational numbers and greater than the other. One of the most interesting results is that there is a set of rational numbers, to be called integers, which obeys the basic axioms of the natural numbers and thus is isomorphic to the set of natural numbers.

Definition 2.1. A fraction is an ordered pair of natural numbers (x,y) denoted by x/y.

Definition 2.2. Two fractions x/y and z/w are said to be equivalent, to be denoted by $x/y \sim z/w$, if and only if $xw = zy$.

Theorem 2.3. The relation $\sim$ is:

i) Reflexive: $a/b \sim a/b$

ii) Symmetric: if $a/b \sim c/d$, then $c/d \sim a/b$

iii) Transitive: if $a/b \sim c/d$ and $c/d \sim e/f$, then $a/b \sim e/f$

Proof. (i). $ab=ab$. Therefore, $a/b \sim a/b$ by 2.2.

(ii). If $a/b \sim c/d$ then $ad = cb$ by 2.2. Thus, $cb = ad$ which implies $c/d = a/b$ by 2.2.

(iii). If $a/b \sim c/d$ and $c/d \sim e/f$ then $ad = cb$ and $cf = ed$ by 2.2.

Hence, $(ad)f = (cb)f$ and $(cf)b = (ed)b$.

Now, $(cb)f = f(cb)$ by 1.8

$= (fc)b$ by 1.10

$= (cf)b$ by 1.8.

Thus, $(cb)f = (cf)b$ and hence $(ad)f = (ed)b$. Similarly, $(ad)f = (af)d$ and $(ed)b = (eb)d$. Therefore, $(af)d = (eb)d$ which implies $af = eb$ by 1.19. Hence, $a/b \sim e/f$ by 2.2. We have shown that the relation $\sim$ defined by $\sim = \{(a/b, c/d): a,b,c,d \in N \text{ and } ad = bc\}$ is an equivalence relation.

Definition 2.4. A rational number is the set of all fractions which are equivalent to a given fraction. If x/y is the given fraction, the rational number will be denoted by $[x/y]$.

Definition 2.5. Two rational numbers $[x/y]$ and $[z/w]$ are said to be equal if and only if every element of $[x/y]$ is an element of $[z/w]$ and every element of $[z/w]$ is an element of $[x/y]$. This definition will be denoted symbolically as follows: $[x/y] = [z/w]$ if and only if $[x/y] \subset [z/w]$ and $[z/w] \subset [x/y]$. Otherwise, $[x/y] \neq [z/w]$.

Theorem 2.6. $[a/b] = [c/d]$ if and only if $a/b \sim c/d$.

Proof. Assume $[a/b] = [c/d]$. Now, $a/b \in [a/b]$ and since $[a/b] = [c/d]$, $a/b \in [c/d]$ by 2.5. Thus $a/b \sim c/d$ by 2.4.

To show the converse assume $a/b \sim c/d$. Let e/f be any element of $[a/b]$. Then $e/f \sim a/b$ by 2.4 which implies $e/f \sim c/d$ by 2.3 (iii). Thus, $e/f \in [c/d]$. Hence, $[a/b] \subset [c/d]$. Similarly, $[c/d] \subset [a/b]$. Therefore, $[a/b] = [c/d]$ by 2.5.

Theorem 2.7 $[a/b] = [c/d]$ if and only if $ad = cb$.

Proof. Assume $[a/b] = [c/d]$. Then $a/b \sim c/d$ by 2.6 and thus $ad = cb$ by 2.2. For the converse assume $ad = cb$. Then $a/b \sim c/d$ by 2.2 and thus $[a/b] = [c/d]$ by 2.6.

Theorem 2.8. The relation = is:

i) Reflexive: $[a/b] = [a/b]$

ii) Symmetric: if $[a/b] = [c/d]$, then $[c/d] = [a/b]$

iii) Transitive: if $[a/b] = [c/d]$ and $[c/d] = [e/f]$, then $[a/b] = [e/f]$.

Proof. (i) $a/b \sim a/b$ by 2.3 (i). Therefore, $[a/b] = [a/b]$ by 2.6.

(ii) If $[a/b] = [c/d]$, then $a/b \sim c/d$ by 2.6. Hence, $c/b \sim a/b$ by 2.3 (ii) and thus $[c/d] = [a/b]$ by 2.6.

(iii) If $[a/b] = [c/d]$ and $[c/d] = [e/f]$, then $a/b \sim c/d$ and $c/d \sim e/f$ by 2.6. Hence, $a/b \sim e/f$ by 2.3 (iii) and so $[a/b] = [e/f]$ by 2.6.

Thus = is an equivalence relation on the set of rational numbers.

Definition 2.9. By the sum of two rational numbers $[a/b]$ and $[c/d]$, to be denoted by $[a/b] \oplus [c/d]$, is meant the following: $[a/b] \oplus [c/d] = [(ad + cb)/bd]$.

Theorem 2.10. $\oplus$ is a binary operation on the set of rational numbers.

Proof. It is obvious that the sum gives a rational number. It must now be shown that the sum is unique; that is, it doesn't depend on the particular fractions used to name the rational numbers. Symbolically, if $[a/b] = [c/d]$ and $[e/f] = [g/h]$ then we wish to show that $[(af + eb)/bf] = [(ch + gd)/dh]$. Since $[a/b] = [c/d]$ and $[e/f] = [g/h]$, $ad = cb$ and $eh = gf$ by 2.7. Hence, $(ad)(fh) = (cb)(fh)$ and $(eh)(bd) = (gf)(bd)$ by 1.19.

Now, $(ad)(fh) = \big(a(df)\big)h$ by 1.10

$= \big(a(fd)\big)h$ by 1.8

$= ((af)d)h$ by 1.10

$= (af)(dh)$ by 1.10

and so $(ad)(fh) = (af)(dh)$. Similarly, $(cb)(fh) = (ch)(bh)$; $(eh)(bd) = (eb)(dh)$, and $(gf)(bd) = (gd)(bf)$. Therefore, $(af)(dh) + (eb)(dh) = (ch)(bf) + (gd)(bf)$. Now $(af)(dh) + (eb)(dh) = (af + eb)(dh)$ and $(ch)(bf) + (gd)(bf) = (ch + gd)(bf)$ by 1.9. Hence, $(af + eb)(dh) = (ch + gd)(bf)$. Therefore, $[(af + eb)/bf] = [(ch + gd)/dh]$ by 2.7 and the theorem is shown.

Theorem 2.11. (Commutative Law of $\oplus$). $[a/b] \oplus [c/d] = [c/d] \oplus [a/b]$.

Proof: $[a/b] \oplus [c/d] = [(ad + cb)/bd]$ by 2.9

$= [(cb + ad)/db]$

$= [c/d] \oplus [a/b]$ by 2.9.

Therefore, $[a/b] \oplus [c/d] = [c/d] \oplus [a/b]$.

Theorem 2.12. (Associative Law of $\oplus$). $([a/b] \oplus [c/d]) \oplus [e/f] = [a/b] \oplus ([c/d] \oplus [e/f])$.

Proof. $([a/b] \oplus [c/d]) \oplus [e/f] = [(ad + cb)/bd] \oplus [e/f]$

$= [((ad + cb)f + e(bd)) / (bd)f]$

$= [(((ad)f + (cb)f) + e(bd)) / b(df)]$

$= [(a(df) + (b(cf) + b(ed))) / b(df)]$

$= [(a(df) + b(cf + ed)) / b(df)]$

$= [a/b] \oplus [(cf + ed)/df]$ by 2.9

$= [a/b] \oplus ([c/d] \oplus [e/f])$ by 2.9.

Thus, $([a/b] \oplus [c/d]) \oplus [e/f] = [a/b] \oplus ([c/d] \oplus [e/f])$.

Definition 2.13. By the product of two rational numbers $[a/b]$ and $[c/d]$, to be denoted by $[a/b] \odot [c/d]$ is meant the following: $[a/b] \odot [c/d] = [(ac)/(bd)]$.

Theorem 2.14. $\odot$ is a binary operation on the set of rational numbers.

Proof. It is obvious that the product is a rational number. To show that the product gives an unique rational number it must be shown that the particular given fraction used to name the rational number is arbitrary; that is, if $[a/b] = [c/d]$ and $[e/f] = [g/h]$ then we must show that $[(ae)/(bf)] = [(cg)/(dh)]$. Since $[a/b] = [c/d]$ and $[e/f] = [g/h]$, ad = cb and eh = gh by 2.7. Thus, (ad)(eh) = (cb)(gf). Now (ad)(eh) = (ae)(dh) and (cb)(gh) = (cg)(bf). Hence, (ae)(dh) = (cg)(bf). Therefore, $[(ae)/(bf)] = [(cg)/(dh)]$ by 2.7 and the theorem is shown.

Theorem 2.15. (Commutative Law of $\odot$). $[a/b] \odot [c/d] = [c/d] \odot [a/b]$.

Proof. $[a/b] \odot [c/d] = [(ac)/(bd)]$ by 2.13

$= [(ca)/(db)]$

$= [c/d] \odot [a/b]$ by 2.13.

Theorem 2.16. (Associative Law of $\odot$). $([a/b] \odot [c/d]) \odot [e/f] = [a/b] \odot ([c/d] \odot [e/f])$.

Proof. $([a/b] \odot [c/d]) \odot [e/f] = [(ac)/(bd)] \odot [e/f]$ by 2.13

$= [((ac)e)/((bd)f)]$ by 2.13

$= [(a(ce))/(b(df))]$

$= [a/b] \odot [(ce)/(df)]$ by 2.13

$= [a/b] \odot ([c/d] \odot [e/f])$ by 2.13.

Thus, $([a/b] \odot [c/d]) \odot [e/f] = [a/b] \odot ([c/d] \odot [e/f])$ and the theorem is proved.

Theorem 2.17. $[a/b] = [(xa)/(xb)]$.

Proof. a(xb) = (ax)b by 1.10

= (xa)b by 1.8

Therefore, $a(xb) = (xa)b$ and so $[a/b] = [(xa)/(xb)]$ by 2.7.

Theorem 2.18. (Distributive Law) . $[a/b] \odot ([c/d] \oplus [e/f]) = [a/b] \odot [c/d] \oplus [a/b] \odot [e/f]$.

Proof. $[a/b] \odot ([c/d] \oplus [e/f]) = [a/b] \odot [(cf + ed)/df]$ by 2.9

$= [(a(cf + ed)) / (b(df))]$ by 2.13

$= [(a(cf) + a(ed)) / (b(df))]$

$= [(b(a(cf) + a(ed)))/(b(b(df)))]$ by 2.17

$= [((ac)(bf) + (ae)(bd)) / ((bd)(bf))]$

$= [(ac)/(bd)] \oplus [(ae)/(bf)]$ by 2.9

$= [a/b] \odot [c/d] \oplus [a/b] \odot [e/f]$ by 2.17.

Therefore, $[a/b] \odot ([c/d] \oplus [e/f]) = [a/b] \odot [c/d] \oplus [a/b] \odot [e/f]$.

Definition 2.19. $[a/b] > [c/d]$ if and only if $ad > cb$. To show this definition is valid it must be shown that it in no way depends upon the particular given fractions used to name the rational numbers. Thus, the following theorem is needed.

Theorem 2.20. If $[a/b] > [c/d]$, $[a/b] = [e/f]$, and $[c/d] = [g/h]$, then $[e/f] > [g/h]$.

Proof. From the hypothesis $ad > cb$, $af = eb$, and $ch = gd$. Hence, (i) $(be)(ch) = (af)(gd)$. Since $ad > cb$ $\exists$/u such that (ii) $ad = cb + u$.

Now, $(eh)(cb) = (be)(ch)$

$= (af)(gd)$ by (i)

$= (gf)(ad)$

$= (gf)(cb + u)$ by (ii)

$= (gf)(cb) + (gf)u$

Hence, $(eh)(cb) > (gf)(cb)$ by 1.11 and thus $eh > gf$ by 1.19.

Therefore, $[e/f] > [g/h]$ by 2.19.

Definition 2.21. $[a/b] < [e/d]$ if and only if $[c/d] > [a/b]$.

Theorem 2.22. Given any two rational numbers $[a/b]$ and $[c/d]$, one and only one of the following must occur: $[a/b] = [c/d]$ or $[a/b] > [c/d]$ or $[a/b] < [c/d]$.

Proof. ad = cb or ad > cb or ad < cb by 1.13. Therefore, if ad=cb then $[a/b] = [c/b]$ by 2.7; if ad > cb then $[a/b] > [c/d]$ by 2.19; if ad < cb then cb > ad by 1.12 and so $[c/d] > [a/b]$ which implies $[a/b] < [c/d]$ by 2.21.

Theorem 2.23. $[a/b] = [c/d]$ or $[a/b] > [c/d]$ or $[a/b] < [c/d]$ if and only if $[a/b] \oplus [x/y] = [c/d] \oplus [x/y]$ or $[a/b] \oplus [x/y] > [a/b] \oplus [x/y]$ or $[a/b] \oplus [x/y] < [c/d] \oplus [x/y]$, respectively.

Proof. Suppose $[a/b] = [c/d]$, then ad = cb. Now,

$$\begin{aligned}
[a/b] \oplus [x/y] &= [(ay + xb)/by] \\
&= [(d(ay + xb)) / (d(by))] \text{ by 2.17.} \\
&= [((ad)y + b(xd)) / (b(dy))] \\
&= [((cb)y + b(xd)) / (b(dy))] \text{ since ad = cb.} \\
&= [(b(cy + xd)) / (b(dy))] \\
&= [(cy + xd)/dy] \text{ by 2.17} \\
&= [c/d] \oplus [x/y].
\end{aligned}$$

And so, $[a/b] \oplus [x/y] = [c/d] \oplus [x/y]$.

Suppose $[a/b] > [c/d]$ then ad > cb. Then (ad)(yy) > (cb)(yy) by 1.19 and (ad)(yy) + (xb)(dy) > (cb)(yy) + (xb)(dy) by 1.18. Now (ad)(yy) = (ay)(dy); (cb)(yy) = (cy)(by); and (xb)(dy) = (xd)(by). Also, (ay)(dy) + (xb)(dy) = (ay + xb)(dy) and (cy)(by) + (xd)(by) = (cy + xd)(by). Hence, (ay + xb)(dy) > (cy + xd)(by) which implies $[(ay + xb)/by] > [(cy + xd)/dy]$ by 2.19. Therefore, $[a/b] \oplus [x/y] > [c/d] \oplus [x/y]$.

If $[a/b] < [c/d]$ then $[c/d] > [a/b]$ and by preceding part $[c/b] \oplus [x/y] > [a/b] \oplus [x/y]$ and so by 2.21 $[a/b] \oplus [x/y] < [c/b] \oplus [x/y]$.

The converse follows immediately from the preceding proof and the fact that the three cases are mutually exclusive and exhaust all possibilities.

Theorem 2.24. $[a/b] = [c/d]$ or $[a/b] > [c/d]$ or $[a/b] < [c/d]$ if and only if $[a/b] \odot [x/y] = [c/d] \odot [x/y]$ or $[a/b] \odot [x/y] > [c/d] \odot [x/y]$ or $[a/b] \odot [x/y] < [c/d] \odot [x/y]$, respectively.

Proof. Suppose $[a/b] = [c/d]$, then ad = cb. Hence (ad)(xy) = (cb)(xy) by 1.19. Now (ad)(xy) = (ax)(dy) and (cb)(xy) = (cx)(by). Thus, (ax)(dy) = (cx)(by) and so $[ax/by] = [cx/dy]$. Therefore, $[a/b] \odot [x/y] = [c/d] \odot [x/y]$.

Suppose $[a/b] > [c/d]$ then ad > cb. Hence, (ad)(xy) > (cb)(xy) by 1.19. Again (ax)(dy) = (ad)(xy) and (cx)(by) = (cb)(xy). Thus (ax)(dy) > (cx)(by) which implies $[ax/by] > [cx/dy]$. Therefore, $[a/b] \odot [x/y] > [c/d] \odot [x/y]$.

If $[a/b] < [c/d]$ then $[c/d] > [a/b]$ and so by preceding part $[c/d] \odot [x/y] > [a/b] \odot [x/y]$. Therefore, $[a/b] \odot [x/y] < [c/d] \odot [x/y]$.

The converse follows immediately from the preceding proof and the fact that the three cases are mutually exclusive and exhaust all possibilities.

Theorem 2.25. Given any rational number $[a/b]$ there exists a rational number $[x/y]$ such that $[x/y] > [a/b]$.

Proof. (a + a)b = ab + ab. Also, ab + ab > ab by 1.17. Therefore (a + a)b > ab and so $[(a + a)/b] > [a/b]$. Let x = a + a and y = b. Then $[x/y] = [(a + a)/b]$ and hence $[x/y] > [a/b]$.

Theorem 2.26. Given any rational number $[a/b]$ there exists a rational number $[x/y]$ such that $[x/y] < [a/b]$.

Proof. ab + aa = aa + ab. Thus, ab < aa + ab by 1.12 and 1.11. Also, aa + ab = a(a + b). Therefore, ab < a(a + b). Hence $[a/(a + b)] < [a/b]$. Let x = a and y = a + b. Then $[x/y] = [a/(a + b)]$ and thus

$[x/y] < [a/b]$.

Theorem 2.27. Given any rational numbers $[a/b]$ and $[c/d]$ such that $[a/b] < [c/d]$, there exists a rational number $[x/y]$ such that $[a/b] < [x/y]$ and $[x/y] < [c/d]$.

Proof. First an $[x/y]$ will be found such that $[a/b] < [x/y]$. From the hypothesis $ad < cb$. Therefore, $\exists/ u$ such that $ad + u = cb$. Thus, $ab + (ad + u) = ab + cb$. Since $ab + (ad + u) = (ab + ad) + u$, $(ab + ad) + u = ab + cb$. Therefore, $ab + ad < ab + cb$. But $ab + ay = a(b + y)$ and $ab + cb = (a + c) b$. Hence $a(b + d) < (a + c)b$ and so $[a/b] < [(a+c)/(b+d)]$.

Now, it will be shown that $[(a+c)/(b+d)] < [c/d]$. Since $ad + u = cb$, $(ad + a) + cd = cb + cd$. But $(ad + u) + cd = (ad + cd) + u$. Therefore, $(ad + cd) + u = cb + cd$ and thus $ad + cd < cb + cd$. Now, $ad + cd = (a+c)d$ and $cb + cd = c(b+d)$. Hence $(a+c)d < c(b+d)$ which implies $[(a+c)/(b+d)] < [c/d]$. Let $x = a+c$ and $y = b+d$. Then, $[x/y] = [(a+c)/(b+d)]$. Hence, $[a/b] < [x/y]$ and $[x/y] < [c/d]$ and the theorem is proved.

Theorem 2.28. Given any rational numbers $[a/b]$ and $[c/d]$ $\exists/$ $[x/y]$ such that $[a/b] \odot [x/y] = [c/d]$.

Proof. The uniqueness of $[x/y]$, if it exists, will be shown first. Assume there exists another rational number $[z/w]$ such that $[a/b] \odot [z/w] = [c/d]$. Then, $[a/b] \odot [x/y] = [a/b] \odot [z/w]$ by 2.8 (iii). Hence $[x/y] = [z/w]$ by 2.24.

To show that such a rational number exists let $x = bc$ and $y = ad$. Then $[x/y] = [(bc)/(ad)]$. Hence, $[a/b] \odot [x/y] = [a/b] \odot [(bc)/(ad)]$

$$= [(a(bc))/(b(ad))]$$

$$= [((ab)c)/((ab)d)]$$

$$= [c/d] \text{ by } 2.17 .$$

$[x/y]$ will be called the quotient of $[c/d]$ by $[a/b]$ and will be denoted as follows: $[x/y] = [(c/d) / (a/b)]$.

Theorem 2.29. If $[a/b] < [c/d]$ $\exists/$ $[x/y]$ such that $[a/b] \oplus [x/y] = [c/d]$.

Proof. As for the uniqueness assume $[z/w]$ also satisfies $[a/b] \oplus [z/w] = [c/d]$. Then $[a/b] \oplus [x/y] = [a/b] \oplus [z/w]$ which implies $[x/y] = [z/w]$ by 2.23.

Now, it will be shown such an $[x/y]$ exists. Since $[a/b] < [c/d]$, $ad < cb$ and so $ad + u = cb$ for some suitable u. Let x=u and y=bd. Then $[x/y] = [u/(bd)]$. Now, $[a/b] + [x/y] = [a/b] + [u/(bd)]$

$$= [(a(bd) + ub)/(b(bd))]$$

$$= [(b(ad + u)) / (b(bd))]$$

$$= [(ad + u)/(bd)] \text{ by 2.17}$$

$$= [(cb)/(bd)] \text{ since } ad + u = cb$$

$$= [c/d] \text{ by 2.17}$$

Thus, $[x/y]$ exists and is unique. $[x/y]$ will be called the difference between $[c/d]$ and $[a/b]$ and will be denoted as follows: $[x/y] = [c/d] - [a/b]$.

Definition 2.30. A rational number is called an integer if and only if it contains an element of the form x/1. This x is uniquely determined for if the rational number contains two such elements say x/1 and y/1, then $x/1 \sim y/1$. Therefore, $x \cdot 1 = y \cdot 1$ and thus $x = y$.

Theorem 2.31. There exists a one-to-one correspondence between the set of integers and the set of natural numbers.

Proof. Set up a correspondence as follows: x and $[x/1]$ correspond for every $x \in N$. To show there corresponds one and only one natural number to each integer, let x and y correspond to $[x/1]$ and $[y/1]$ respectively with $[x/1] = [y/1]$. Then $x \cdot 1 = y \cdot 1$ and so $x=y$.

For the converse, let x and y correspond to $[x/1]$ and $[y/1]$ respectively, with $x=y$. Then $x \cdot 1 = y \cdot 1$ which implies $[x/1] = [y/1]$. And so the theorem is proved.

Theorem 2.32. The integers obey the axioms of natural numbers if $[x'/1]$ is assigned the role of the successor of $[x/1]$ and $[1/1]$ plays the role of 1; i.e.,

Axiom 1.II. If $[x/1] = [y/1]$ then $[x'/1] = [y'/1]$.

Axiom 2.II. There exists an integer $[1/1]$ such that $[x'/1] \neq [1/1]$.

Axiom 3.II. If $[x'/1] = [y'/1]$, then $[x/1] = [y/1]$.

Axiom 4.II. If a set I of integers contains $[1/1]$ and it contain $[x'/1]$ whenever it contains $x/1$, then I contains all the integers.

Proof. Since $[x/1] = [y/1]$, $x \cdot 1 = y \cdot 1$. Thus $x=y$ and by Axiom 1.I, $x'=y'$. Hence, $x' \cdot 1 = y' \cdot 1$ which implies $[x'/1] = [y'/1]$.

The existence of $[1/1]$ is obvious. To show $[x'/1] \neq [1/1]$ the proof is by contradiction. Suppose $[x'/1] = [1/1]$. Then $x' \cdot 1 = 1 \cdot 1$ which implies $x'=1$. But by Axiom 2.I, $x' \neq 1$. Hence, $[x'/1] \neq [1/1]$.

From the hypothesis $x' \cdot 1 = y' \cdot 1$. Therefore, $x' = y'$ and $x = y$ by Axiom 3. Hence, $x \cdot 1 = y \cdot 1$ and so $[x/1] = [y/1]$.

Let M be the set of all natural numbers x such that $[x/1] \in I$. From the hypothesis $[1/1] \in I$, thus $1 \in M$. Also, $x' \in M$ whenever $x \in M$ since if $[x/1] \in I$, $[x'/1] \in I$. Hence, M is the same set as Nand so contains all the natural numbers. Thus, I contains all the integers.

With $[1/1]$ playing the role of 1 and $[x'/1]$ being the unique successor of $[x/1]$ it can be shown that the set of integers is ismorphic to the set of natural numbers.

CUTS

Cuts will be defined in terms of sets of rational numbers. Their basic properties will be established and again it will be pointed out that a subset of the set of cuts, under appropriate definitions, is isomorphic to the integers and thus to the natural numbers.

Definition 3.1. A set of rational numbers is called a cut if and only if:

1) it contains a rational number, but not all rational numbers;

2) every rational number of the set is less than every rational number not in the set;

3) it does not contain a greatest rational number.

Cuts will be denoted by upper case letters such as W,X,Y,Z.

Definition 3.2. Two cuts X and Y are equal; i.e., $X=Y$, if and only if $X \subset Y$ and $Y \subset X$. Otherwise, $X \neq Y$.

Theorem 3.3. The relation = is:

i) Reflexive: $X=X$.

ii) Symmetric: $X=Y$, then $Y=X$

iii) Transitive: $X=Y$ and $Y=Z$, then $X=Z$

Proof. Trivial.

And so = is an equivalence relation on the set of cuts.

Theorem 3.4. If $[a/b] \notin X$ and if $[c/d] > [a/b]$, then $[c/d] \notin X$.

Proof. The proof is by contradiction. Assume $[c/d] \in X$. Then $[c/d] < [a/b]$ by 3.1(2), and this is a contradiction of the hypothesis. Thus, $[c/d] \notin X$.

Theorem 3.5. If $[a/b] \in X$ and $[c/d] < [a/b]$, then $[c/d] \in X$.

Proof. Assume $[c/d] \notin X$. Then, $[a/b] < [c/d]$ by 3.1(2) and this contradicts the hypothesis. Thus, $[c/d] \in X$.

Theorem 3.6. Theorem 3.5 and definition 3.1(2) are equivalent.

Proof. That definition 3.1(2) implies Theorem 3.5 was shown in the proof of Theorem 3.5. To show that Theorem 3.5 implies Definition 3.1(2) let $[a/b]$ be any element of X and $[c/d]$ be any element not in X. Obviously, $[a/b] \neq [c/d]$. Assume $[c/d] < [a/b]$. By 3.6 since $[a/b] \in X$, $[c/d] \in X$ and this contradicts the hypothesis. Hence, $[a/b] < [c/d]$.

Theorem 3.5 may now be used in place of definition 3.1(2) in showing that a set of rational numbers is a cut.

Definition 3.7. $X > Y$ if and only if there exists $[a/b]$ such that $[a/b] \in X$ and $[a/b] \notin Y$.

Definition 3.8. $X < Y$ if and only if $Y > X$.

Theorem 3.9. Given X and Y, one and only one of the following can occur; $X=Y$ or $X > Y$ or $X < Y$.

Proof. To show that only one of the three cases can occur let $X=Y$ and $X < Y$. Then, $Y < Y$ and this contradicts Theorem 3.3(i). Similarly, $X=Y$ and $X > Y$ cannot occur simultaneously. If $X > Y$ and $X < Y$, then there exists $[a/b]$ such that $[a/b] \notin X$ and $[a/b] \notin Y$, and there exists $[c/d]$ such that $[c/d] \in X$ and $[c/d] \notin Y$. Thus $[a/b] > [c/d]$ and $[a/b] < [c/d]$ by 3.1(2) and this contradicts Theorem 2.22. So, only one of the cases can occur.

To show that one of the cases must occur we note that either $X=Y$ or $X \neq Y$. If $X \neq Y$ there exists $[a/b]$ such that $[a/b] \in X$ and $[a/b] \notin Y$ which implies $X > Y$ by 3.7; or, there exists $[c/d]$ such that $[c/d] \notin X$ and $[c/d] \in Y$ which implies $Y > X$ by 3.7 and so by 3.8, $X < Y$. Hence, one of the three cases must occur.

Theorem 3.10. If $X < Y$ and $Y < Z$, then $X < Z$.

Proof. Trivial.

Definition 3.11. By the sum of X and Y, denoted by X+Y, is meant the set of all rational numbers which are expressible in the form $[a/b] + [c/d]$ where $[a/b] \in X$ and $[c/d] \in Y$.

We note that although the above symbol is the same as the addition symbol for natural numbers. the corresponding operations are not the same. This symbol will from now on be used to represent the binary operation addition on any set to avoid cumbersome notation and it will be clear from the context which is meant. Similarly, from now on $\cdot$ will represent the binary operation multiplication on any set and usually will be omitted.

Theorem 3.12. + is a binary operation on the set of cuts.

Proof. To establish this theorem, the following lemma is needed.

Lemma 3.13. No element of X + Y can be written as $[a/b] + [c/d]$ where $[a/b]$ is any element not in X and $[c/d]$ is any element not in Y.

Proof. Let $[x/y]$ be any element of X and $[z/w]$ be any element of Y. Then $[x/y] < [a/b]$ and $[z/w] < [c/d]$ by 3.1(2) and this implies that $[x/y] + [z/w] < [a/b] + [c/d]$. Since all elements were arbitrary the lemma is proved.

Now to show that X + Y is a cut

1) Let X and Y be any two cuts with $[a/b] \in X$ and $[c/d] \notin Y$. Then, $[a/b] + [c/d] \in X + Y$ by 3.11. Thus, X + Y has an element. If $[x/y] \notin X$ and $[z/w] \notin Y$, then $[x/y] + [z/w] \notin X + Y$ by 3.13. Hence, there is an element not in X + Y.

2) Given any $[x/y] \in X + Y$ then $[x/y] = [a/b] + [c/d]$ where

$[a/b] \in X$ and $[c/d] \in Y$ by 3.11. Let $[z/w]$ be any element less than $[x/y]$. We note that if we can show that $[z/w]$ is expressible as the sum of two rational numbers contained respectively in X and Y, then Theorem 3.5 is satisfied and thus this implies Definition 3.1(2) by Theorem 3.6.

Now, $[z/w] = ([a/b] + [c/d])([z/w]/([a/b] + [c/d]))$ by 2.28. Also, $[a/b] + [c/d] = ([a/b] + [c/d])[1/1]$. Since $[z/w] < [a/b] + [c/d]$, $([a/b] + [c/d])([z/w]/([a/b] + [c/d])) < ([a/b] + [c/d])[1/1]$. Thus; $[z/w]/([a/b] + [c/d]) < [1/1]$ by 2.24. Now, $[a/b]([z/w]/([a/b] + [cd])) < [a/b][1/1] = [a/b]$ and so is an element of X. Also, $[c/d] \cdot ([z/w]/([a/b] + [c/d])) < [c/d][1/1] = [c/d]$ and so is an element of Y. Hence, $[z/w] = ([a/b] + [c/d])([z/w]/([a/b] + [c/d])) = [a/b] \cdot ([z/w]/([a/b] + [c/d])) + [c/d]([z/w]/([a/b] + [c/d]))$ by 2.18. Therefore, $[z/w]$ can be expressed as the sum of elements of X and Y respectively and thus $[z/w] \in X + Y$. Thus, part(2) in Definition 3.1 is satisfied.

3) Given any $[x/y] \in X + Y$ then $[x/y] = [a/b] + [c/d]$ where $[a/b] \in X$ and $[c/d] \in Y$. There exists $[z/w] \in X$ such that $[z/w] > [a/b]$ since X is a cut. Hence, $[a/b] + [c/d] < [z/w] + [c/d]$ by 2.25. Since $[z/w] + [c/d]$ is obviously an element of X + Y and $[x/y]$ was any element of X + Y, X + Y has no greatest element and part(3) in Definition 3.1 is satisfied. Hence, X + Y is a cut.

X + Y is unique since each of its elements is an unique sum of rational numbers.

Theorem 3.13. $X + Y > X$.

Proof. Let $[c/d]$ be any element of Y. Now there exist $[a/b] \in X$ and $[x/y] \in X$ such that $[a/b] - [x/y] = [c/d]$. Thus, $[a/b] = ([a/b] - [x/y]) + [x/y] = [c/d] + [x/y]$. Thus $[c/d] + [x/y] \notin X$

and is an element of $X + Y$. Hence $X + Y > X$ by 3.7.

Theorem 3.14. $X = Y$ or $X > Y$ or $X < Y$ if and only if $X + Z = Y + Z$ or $X + Z > Y + Z$ or $X + Z < Y + Z$ respectively.

Proof. If $X = Y$ then obviously $X + Z = Y + Z$: $X > Y$ implies there exists $[a/b]$ such that $[a/b] \in X$ and $[a/b] \notin Y$. Choose $[x/y]$ such that $[x/y] < [z/w]$ where $[z/w] \in X$ by 2.26. Now there exists $[u/v] \notin Z$ and $[r/s] \in Z$ such that $[u/v] - [r/s] = [z/w] - [x/y]$.

$$\begin{aligned} \text{Thus, } [u/v] + [x/y] &= ([u/v] - [r/s]) + ([r/s] + [x/y]) \\ &= ([z/w] - [x/y]) + ([r/s] + [x/y]) \\ &= [z/w] + [r/s]. \end{aligned}$$

Hence, $[z/w] + [r/s] \in X + Z$ and $[u/v] + [x/y] \notin Y + Z$. Thus, $X + Z > Y + Z$.

If $X < Y$ then $Y > X$ by 3.8 which implies that $Y + Z > X + Z$ by above and so $X + Z < Y + Z$ by 3.8.

The converse follows immediately from the preceding proof and the fact that the cases are mutually exclusive and exhaust all possibilities.

Theorem 3.15. $X + Y = Y + X$

Proof. Trivial.

Theorem 3.16. $(X+Y) + Z = X + (Y+Z)$.

Proof. Trivial.

Theorem 3.17. If $X > Y$, $\exists! Z$ such that $X = Y + Z$.

Proof. Z is unique for if T is also a solution then $Y + T = Y + Z$ which implies $T = Z$ by 3.14.

To show such an Z exists, look at the set of all rational numbers expressible in the form $[a/b] - [c/d]$ where $[a/b] \in X$, $[c/d] \notin Y$, and $[a/b] > [c/d]$. This set is a cut since:

1) $X > Y$ implies there exists $[a/b]$ such that $[a/b] \in X$ and $[a/b] \notin Y$. Let $[c/d]$ be any element of X such that $[c/d] > [a/b]$ by 3.1(3). Thus, $[c/d] - [a/b]$ exists and is an element of the set. Let $[x/y]$ be any element not in X, and let $[z/w]$ be any element in the set. Then $[z/w] = [u/v] - [r/s]$ where $[u/v] \in X$, $[r/s] \notin Y$, and $[u/v] > [r/s]$.

Now, $[u/v] - [r/s] < ([u/v] - [r/s]) + [r/s]$

$= [u/v]$ by 2.29

$< [x/y]$ by 1.3(2).

Hence, $[x/y]$ exists since X is a cut and is not an element of the set, and so property (1) in 3.1 is satisfied.

2) Let $[z/w]$ be any element of the set. Then $[z/w] = [a/b] - [c/d]$ where $[a/b] \in X$, $[c/d] \notin Y$ and $[a/b] > [c/d]$. Let $[x/y]$ be any element such that $[x/y] < [z/w]$. Now, $[x/y] + [c/d] < ([a/b] - [c/d]) + [c/d]$ by 2.23. Thus, $x/y + z/w = c/d$.

Thus $[x/y] + [c/d] \in X$ by 3.5. Now, $[x/y] + [c/d] = [x/y] + [c/d]$ implies $[x/y] = ([x/y] + [c/d]) - [c/d]$ where $[x/y] + [c/d] \in X$, $[c/d] \notin Y$ and $[x/y] + [c/d] > [c/d]$. Hence $[x/y]$ belongs to the set and by 3.6 part (2) of Definition 3.1 is shown.

3) Given any $[x/y]$ in the set. Then $[x/y] = [a/b] - [c/d]$ where $[a/b] \in X$, $[c/d] \notin Y$ and $[a/b] > [c/d]$. Let $[z/w] \in X$ such that $[z/w] > [a/b]$. Then, $([z/w] - [c/d]) + [c/d] > ([a/b] - [c/d]) + [c/d]$ which implies $[z/w] - [c/d] > [a/b] - [c/d]$ by 3.14. Hence, no greatest element exists and part (3) in Definition 3.1 is shown. Thus our set is a cut and it will be denoted by Z.

It remains to show that Z is the cut which satisfies the relation $X = Y + Z$.

Show $Y + Z \subset X$. Let $[x/y] \in Y + Z$, then $[x/y] = [a/b] + ([c/d] - [e/f])$ where $[a/b] \in Y$, $[c/d] \in X$, $[e/f] \notin Y$, and $[c/d] > [e/f]$. Now, $[a/b] < [e/f]$ by 3.1(2) which implies $[a/b] + ([c/d] - [e/f]) < [e/f] + ([c/d] - [e/f])$ by 2.23.

$= [c/d]$ by 2.29.

Hence $[x/y] \in X$ by 3.5 and so $Y + Z \subset X$.

Show $X \subset Y + Z$. Let $[x/y] \in X$ and $[x/y] \notin Y$. Since X is a cut $[a/b] \in X$ $[a/b] > [x/y]$. For the cut Y $\exists [u/v] \notin Y$ and $[z/w] \in Y$ such that $[u/v] - [z/w] = [a/b] - [x/y]$. Thus, $[u/v] + [x/y] = [a/b] + [z/w]$. Now, $([u/v] + ([x/y] - [z/w])) + [z/w] = [u/v] + (([x/y] - [z/w]) + [z/w])$

$= [u/v] + [x/y]$

$= [a/b] + [z/w]$.

Hence, $[u/v] + ([x/y] - [z/w]) = [x/y]$ by 2.23 which implies $[a/b] - [u/v] = [x/y] - [z/w]$. Since $[x/y] - [z/w]$ exists, $[a/b] - [u/v]$ exists. Let $[a/b] - [u/v] = [r/s]$. Then $[u/v] = [a/b] - [r/s]$. Now, $[a/b] < [a/b] + [r/s]$. Hence, $([a/b] - [r/s]) + [r/s] < [a/b] + [r/s]$ which implies $[a/b] - [r/s] < [a/b]$ by 2.23. Thus, $[u/v] < [a/b]$ and so $[x/y] = ([x/y] - [z/w]) + [z/w]$

$= ([a/b] - [u/v]) + [z/w]$

$= [z/w] + ([a/b] - [u/v])$

is an element of $Y + Z$. Hence, $X \subset Y + Z$. Therefore, $X = Y + Z$ by 3.2.

The cut Z is denoted by X - Y and is called the difference X minus Y.

Definition 3.18. By the product of X and Y, denoted by XY, is meant the set of all rational numbers which are expressible in the form $[a/b]\,[c/d]$ where $[a/b] \in X$ and $[c/d] \in Y$.

Theorem 3.19. $\cdot$ is a binary operation on the set of cuts.

Proof. To prove this theorem the following lemma is needed.

Lemma 3.20. No element of XY can be written as $[a/b]\,[c/d]$ where $[a/b] \notin X$ and $[c/d] \notin Y$.

Proof. Let $[x/y]$ be any element of X and $[z/w]$ be any element of Y. Then $[x/y] < [a/b]$ and $[z/w] < [c/d]$. Hence, $[x/y]\,[z/w] < [a/b]\,[c/d]$. Since all elements were arbitrary, the lemma is proved.

Now, to show that XY is cut.

1) Since X and Y are cuts, there exists $[a/b] \in X$ and $[c/d] \in Y$. Therefore, $[a/b]\,[c/d]$ exists and is an element of the set. Let $[x/y]$ be any element not in X and $[z/w]$ be any element not in Y. Then, $[x/y]\,[z/w]$ exists and is not an element of the set by 3.20.

2) Let $[z/w] \in XY$ then $[z/w] = [a/b]\,[c/d]$ where $[a/b] \in X$ and $[c/d] \in Y$. Let $[x/y]$ be any element less than $[z/w]$. Then $\exists!\ [u/v]$ such that $[x/y]\,[u/v] = [a/b]\,[c/d]$ by 2.28. Thus, $[x/y] = \left([a/b]\,[c/d]\right)/[u/v]$. Now, $\left([a/b]\,[c/d]\right)/\left([u/v]\,[u/v]\right)$

$= [a/b]\,[c/d]$

$= [a/b]\left(\left([c/d]/[u/v]\right)[u/v]\right)$

$= \left([a/b]\left([c/d]/[u/v]\right)\right)[u/v]$ by 2.16.

Hence, $\left([a/b]\,[c/d]\right)/[u/v] = [a/b]\left([c/d]/[u/v]\right)$ by 2.26.

Also, $[x/y] = [a/b]\left([c/d]/[u/v]\right) < [a/b]\,[c/d]$. Hence $[c/d]/[u/v]$ $[c/d]$ and so $[c/d]/[u/v] \in Y$. Since $[a/b] \in X$, $[x/y] \in XY$ and so part (2) in definition 3.1 is satisfied.

3) Let $[a/b] \in X$ and $[c/d] \in Y$. Then there exists $[x/y] \in X$ such that $[x/y] > [a/b]$. Hence, $[x/y]\,[c/d] \in XY$ and $[x/y]\,[c/d] > [x/y]\,[a/b]$ by 2.26.

Hence, the set XY is a cut.

XY is unique since each of its elements is a unique product of rational numbers.

Theorem 3.21. XY = YX.

Proof. Trivial.

Theorem 3.22. (XY)Z = X(YZ)

Proof. Trivial

Theorem 3.23. X(Y+Z) = XY + XZ.

Proof. To show $X(Y+Z) \subset XY + XZ$ let $[x/y]$ be any element of X(Y+Z). Then $[x/y] = [a/b]([c/d] + [e/f])$ where $[a/b] \in X$, $[c/d] \in Y$ and $[e/f] \in Z$. Now $[a/b]([c/d] + [e/f]) = [a/b][c/d] + [a/b][c/f]$ by 2.18. Thus, $[x/y] \in XY + XZ$.

To show $XY + XZ \subset X(Y+Z)$ let $[x/y] \in XY + XZ$. Then $[x/y] = [a/b] \cdot [c/d] + [e/f][g/h]$ where $[a/b] \in X$, $[c/d] \in Y$, $[e/f] \in X$, $[g/h] \in Z$. Choose the greater rational number of $[a/b]$ and $[e/f]$. Suppose $[a/b]$ is the greater. Then $[e/f] < [a/b]$ implies $[e/f][g/h] < [a/b][g/h]$. Hence, $[a/b][c/d] + [e/f][g/h] < [a/b][c/d] + [a/b][g/h]$

$$= [a/b]([c/d] + [g/h]) \text{ by 2.18.}$$

Thus, $[x/y] \in X(Y+Z)$ and hence, $XY + XY \subset X(Y+Z)$. Therefore, by 3.2 the theorem is proved.

Theorem 3.24. Given $[r/s]$, the set of all rational numbers less than $[r/s]$ constitutes a cut.

Proof.1) By 2.28 there exists $[z/w]$ such that $[z/w] < [r/s]$. So the set has an element. The number $[r/s]$ exists and doesn't belong to the set.

2) Let $[a/b]$ belong to the set. Let $[x/y]$ be any rational number less than $[a/b]$. Since $[a/b] < [r/s]$ and $[x/y] < [a/b]$,

$[x/y] < [r/s]$. Hence, $[x/y]$ belongs to the set.

3) Let $[a/b]$ belong to the set then $[a/b] < [r/s]$. By 2.27 there exists $[x/y]$ such that $[a/b] < [x/y] < [r/s]$. Thus, the set contains no greatest number. Hence, the set is a cut.

Definition 3.25. The cut in Theorem 3.24 will be called a rational cut and will be denoted by $[r/x]^*$. In general rational cuts will be denoted by rational numbers with asterisks with the exception that in the following development $[1/1]^*$ will be denoted by 1.

Theorem 3.26. $X=Y$ or $X>Y$ or $X<Y$ if and only if $XZ = YZ$ or $XZ > YZ$ or $XZ < YZ$ respectively.

Proof. The following lemma is used in the proof of this theorem.

Lemma 3.27. If $X = Y+Z$, then $X>Y$.

Proof. Either $X=Y$ or $X>Y$ or $X<Y$ by 3.9. If $X=Y$ then $Y=Y+Z$ and this contradicts 3.13. If $X<Y$ then $\exists/T$ such that $X+T = Y$ by 3.17 and 3.8. Hence $X = (X+T)+Z$

$= X + (T+Z)$ by 3.16

which again contradicts 3.13. Thus $X>Y$.

Now, suppose $X=Y$ then obviously $XZ = YZ$.

If $X>Y$ $\exists/T$ such that $X = Y+T$. Thus $XZ = (Y+T)Z = YZ + TZ$ by 3.23. Hence, $XZ > YZ$ by 3.27.

If $X<Y$ then $Y>X$ which implies $YZ>XZ$ which implies $XZ<YZ$.

The converse follows immediately from the preceding proof and the fact that the three cases are mutually exclusive and exhaust all possibilities.

Theorem 3.28. $X \cdot 1 = X$.

Proof. To show that $X \cdot 1 \subset X$ let $[z/w] \in X \cdot 1$. Then $[z/w] = [x/y][a/b]$ where $[x/y] \in X$ and $[a/b] \in 1$. Since $[a/b] \in 1$, $[a/b] < [1/1]$. Thus,

$[x/y]\,[a/b] < [x/y]\,[1/1] = [x/y]$. Hence, $[z/w] \in X$ and $X \cdot 1 \subset X$.

To show $X \subset X \cdot 1$ let $[x/y] \in X$. Since X is a cut there exists $[z/w] \in X$ such that $[x/y] < [z/w]$. Now, $[1/1] / [z/w]\,[x/y] = [x/y] / [z/w]$. Thus, $[x/y] / [z/w] = ([1/1] / [z/w])\,[x/y] < ([1/1] / [z/w])\,[z/w] = [1/1]$. Hence, $[x/y]/[z/w] \in 1$. Therefore, $[x/y] = [z/w]\,([x/y] / [z/w]) \in X \cdot 1$. Hence, $X \subset X \cdot 1$. Thus, $X \cdot 1 = X$.

Theorem 3.29. Given X, $\exists/Y$ such that $XY = 1$.

Proof. The uniqueness of Y is easily established since if Z is also a solution then $XY = XZ$ which implies $Y=Z$ by 3.26.

Consider the set of all rational numbers of the form $[1/1] / [x/y]$ where $[x/y] \notin X$, excepting the least rational number which is not an element of X, if one exists.

1) Let $[x/y] \notin X$. The rational number $[(x+x)/y] > [x/y]$ since $(x+x)y = xy + xy > xy$. Thus, $[(x+x)/y] \notin X$ by 3.4 and is not the least such element. So $[1/1] / [(x+x)/y]$ belongs to the set. Let $[a/b] \in X$ then $[1/1] / [a/b]$ is not an element of the set for if it were then $[1/1] / [a/b] = [1/1] / [c/d]$ where $[c/d] \notin X$. Hence, $([c/d]\;[a/b])([1/1] / [a/b]) = ([c/d]\;[a/b])([1/1] / [c/d])$ which implies $[a/b] = [c/d]$. Hence $[a/b] \notin X$ which contradicts hypothesis that $[a/b] \in X$.

2) Let $[1/1] / [x/y]$ belong to the set where $[x/y] \notin X$ and is not the least such element, if one exists. Let $[z/w] < [1/1] / [x/y]$. Now,

$$
\begin{aligned}
[z/w]\;[w/z] &= [(zw)/(wz)] \\
&= [(wz)\cdot 1/(wz\cdot 1)] \\
&= [1/1]
\end{aligned}
$$

Thus, $[z/w] = [1/1] / [w/z]$ and so $[1/1] / [w/z] < [1/1] / [x/y]$. Hence,

$([w/z]\ [x/y])([1/1]/[w/z]) < ([w/z]\ [x/y])([1/1]/[x/y])$ which implies $[x/y] < [w/z]$. Therefore, $[w/z] \notin X$ and is not the least such element. Hence $[z/w]$ is an element of the set.

3) Let $[x/y] \notin X$ where $[x/y]$ is not the least such element, if one exists. Now there exists $[a/b]$ such that $[a/b] < [x/y]$. By 2.27 there exists $[c/d]$ such that $[a/b] < [c/d]$ and $[c/d] < [x/y]$. Thus, $[c/d] \notin X$ and is not the least such element. Since $[c/d] < [x/y]$,

$$\Big(([1/1]/[x/y])\ ([1/1]/[c/d])\Big)\ [c/d] < \Big(([1/1]/[x/y])\ ([1/1]/[c/d])\Big)\ [x/y]$$

implies $[1/1]/[x/y] < [1/1]/[c/d]$. Hence no greatest element of the set exists. The set is a cut and will be denoted by Y.

It remains to show that XY = 1. To show $XY \subset 1$ let $[x/y]$ be any element of XY then $[x/y] = [a/b]([1/1]/[c/d])$ where $[a/b] \in X$ and $[1/1]/[c/d] \in Y$. Thus, $[c/d] \notin X$ and so $[a/b] < [c/d]$. Hence, $[a/b] \cdot ([1/1]/[c/d]) = [a/b]/[c/d] < [1/1]$ and so $[x/y] \in 1$. Thus, $XY \subset 1$.

To show $1 \subset XY$ let $[a/b]$ be any element of 1. Thus, $[a/b] < [1/1]$. Now, there exists $[x/y] \notin X$ and $[z/w] \in X$ such that $[x/y] - [z/w] = ([1/1] - [a/b])[c/d]$ where $[c/d] \in X$. Since $[x/y] > [c/d]$,

$$\begin{aligned} [x/y] - [z/w] &< ([1/1] - [a/b])[x/y] \\ &= [1/1]\ [x/y] - [a/b]\ [x/y] \\ &= [x/y] - [a/b]\ [x/y]. \end{aligned}$$

Thus, $([x/y] - [z/w]) + ([z/w] + [a/b]\ [x/y]) = [x/y] + [a/b] \cdot [x/y] < ([x/y] - [a/b]\ [x/y]) + ([z/w] + [a/b]\ [x/y]) = [x/y] + [z/w]$ which implies $[a/b]\ [x/y] < [z/w]$. Thus, $([a/b]\ [x/y])\ [1/1]/[a/b] = [x/y] < [z/w]\ ([1/1]/[a/b]) = [z/w]/[a/b]$. Hence, $[z/w]/[a/b] \notin X$ and is not the least such element. Therefore, $[a/b] = [z/w]\ ([1/1]/([z/w]/[a/b]))$ where $[z/w] \in X$ and $[z/w]/[a/b] \notin X$. Hence, $[a/b] \in XY$ and $1 \subset XY$.

And so $XY = 1$.

Theorem 3.30. Given X and Y, $\exists/Z$ such that $XZ = Y$.

Proof. The uniqueness is obvious. By 3.29 $\exists/W$ such that $XW = 1$. Then $Z = WY$ is the solution since $XZ = X(WY) = (XW)Y = 1 \cdot Y = Y$.

Z is called the quotient of Y by X and is denoted by Y/X.

Definition 3.31. A cut of the form $[x/1]*$ is called an integral cut.

Theorem 3.32. $[a/b] = [c/d]$ or $[a/b] > [c/d]$ or $[a/b] < [c/d]$ if and only if $[a/b]* = [c/d]*$ or $[a/b]* > [c/d]*$ or $[a/b]* < [c/d]*$ respectively.

Proof. If $[a/b] = [c/d]$, then obviously $[a/b]* = [c/b]*$.

If $[a/b] > [c/d]$ then $[c/d] \in [a/b]*$. By 3.24 and 3.25 $[c/d] \notin [c/d]*$. Hence, $[a/b]* > [c/d]*$.

If $[a/b] < [c/d]$ then $[c/d] > [a/b]$. Thus, by above proof $[c/d]*$ $[a/b]*$ and so $[a/b]* < [c/d]*$.

The converse follows immediately from the preceding proof since the three cases are mutually exclusive and exhaust all possibilities.

Theorem 3.33. The integral cuts satisfy the axioms of the natural numbers if the role of 1 is assigned to 1 and if $([x/1]*)' = [x'/1]*$; i.e.,

Axiom 1.III. If $[x/1]* = [y/1]*$ then $[x'/1]* = [y'/1]*$.

Axiom 2.III. There exists an integral cut 1 such that $[x'/1]* \neq 1$.

Axiom 3.III. If $[x'/1]* = [y'/1]*$, then $x/1* = y/1*$.

Axiom 4.III. Let M* denote a set of integral cuts possessing the following properties:

a) $1 \in M*$, and

b) if $[x/1]* \in M*$, then $([x/1]*)' \in M*$

Then M* contains all integral cuts.

Proof. Since $[x/1]* = [y/1]*$, $[x/1] = [y/1]$ by 3.32. Thus,

$[x'/1] = [y'/1]$ by 2.32 Axiom 1.II. And so $[x'/1]^* = [y'/1]^*$ by 3.32.

The existence of 1 is obvious. To show $[x'/1]^* \neq 1$ suppose $[x'/1]^* = 1$. Then $[x'/1] = [1/1]$ and this contradicts 2.32, Axiom 2.II. Hence, $[x'/1]^* \neq 1$.

Since $[x'/1]^* = [y'/1]^*$, $[x'/1] = [y'/1]$. Thus by 2.32 Axiom 3.II., $[x/1] = [y/1]$ and so $[x/1]^* = [y/1]^*$.

Let M be the set of all $[x/1]$ for which $[x/1]^* \in M^*$. $[1/1] \in M$ since $1 \in M^*$. Also, $[x'/1] \in M$ whenever $[x/1] \in M$ since $([x/1]^*)' \in M^*$ whenever $[x/1]^* \in M^*$. Hence, M contains all integers and M* contains all integral cuts.

With 1 playing the role of 1 and $[x'/1]^*$ being the unique successor of $[x/1]^*$ it can be shown that the set of integral cuts is isomorphic to the set of integers.

Theorem 3.34. A cut is rational if and only if there exists a least element $[a/b]$ which is not an element of the cut. $[a/b]^*$ is then the cut.

Proof. Suppose the cut is rational. Denote the cut by $[a/b]^*$. Now $[a/b] \notin [a/b]^*$ and is the least such element, for if there exists another such element $[c/d]$ such that $[c/d] < [a/b]$ then $[c/d] \in [a/b]^*$.

Suppose there exists a least element $[a/b]$ which is not an element of the cut. Then every $[x/y] \geq [a/b]$ is not an element of the cut and every $[z/w] < [a/b]$ belongs to the cut. Hence by definition $[a/b]^*$ is the cut.

Theorem 3.35. Let X be a cut. Then $[a/b] \in X$ if and only if $[a/b]^* < X$, and hence is not an element of X if and only if $[a/b]^* \geq X$.

Proof. If $[a/b] \in X$ then $[a/b] \notin [a/b]^*$. Hence, $[a/b]^* < X$.

If $[a/b] \notin X$ and is the least such element then $[a/b]^* = X$ by 3.34.

If $[a/b] \notin X$ and is not the least such element choose $[x/y] \notin X$ such that $[x/y] < [a/b]$. Thus $[x/y] \in [a/b]^*$. Hence, $[a/b]^* > X$.

The converse follows immediately from the preceding proof and the fact that the three cases are mutually exclusive and exhaust all possibilities.

Theorem 3.36. If $X < Y$ there exists $[a/b]^*$ such that $X < [a/b]^* < Y$.

Proof. $X < Y$ implies there exists $[x/y]$ such that $[x/y] \notin X$ and $[x/y] \in Y$. By Theorem 3.35, $X \leq [x/y]^* < Y$. Choose $[a/b] \in Y$ such that $[x/y] < [a/b]$. Then $[x/y]^* < [a/b]^*$ and thus $X \leq [x/y]^* < [a/b]^* < Y$ which implies $X < [a/b]^* < Y$.

Theorem 3.37. For each X, $YY = X$ has an unique solution.

Proof. To show the uniqueness assume T and Z are solutions with $T < Z$. Then $TT < ZT$ and $ZT < ZZ$. And so, $TT < ZZ$. Hence the solution is unique, if it exists.

To show the solution exists consider the set of all $[a/b]$ such that $[a/b]\,[a/b] \in X$. This set is a cut for :

1) If $[a/b] \in 1$ and $[a/b] \in X$ then $[a/b]\,[a/b] \in 1 \cdot X = X$. Hence X contains an element of the form $[a/b]\,[a/b]$ and our set has an element.

If $[a/b] \notin 1$ and $[a/b] \notin X$ then $[a/b]\,[a/b] \notin 1 \cdot X = X$ by 3.20. Thus the set does not contain all rational numbers.

2) Let $[a/b]$ be any element less than $[x/y]$ where $[x/y]\,[x/y] \in X$. Then $[a/b]\,[a/b] < [x/y]\,[x/y]$ and so $[a/b]\,[a/b] \in X$. Hence $[a/b]$ belongs to the set.

3) Let $[z/w]$ be any element of X then $[z/w] = [x/y]\,[x/y]$. Choose $[a/b]$ such that $[a/b] \in 1$ and $[a/b]\Big([x/y] + \big([x/y] + [1/1]\big)\Big) + [x/y]\,[x/y] \in X$. Now $[x/y] + [a/b] > [x/y]$. Hence, $\big([x/y] + [a/b]\big)\big([x/y] + [a/b]\big) = \big([x/y] + [a/b]\big)[x/y] + \big([x/y] + [a/b]\big) \cdot [a/b] < \big([x/y]\,[x/y] + [a/b]\,[x/y]\big) + \big([x/y] + [1/1]\big)\,[a/b] = [x/y] \cdot$

$[x/y] + ([a/b]\ [x/y] + ([x/y] + [1/1])\ [a/b]) = [x/y]\ [x/y] +$
$[x/y] + ([x/y] + ([x/y] + [1/1]))\ [a/b] \in X.$

Hence, $([x/y] + [a/b])([x/y] + [a/b]) \in X$ and the set contains no greatest number. Denote this set by y.

It remains to show that $YY = X$.

Suppose $YY > X$. Then there exists $[x/y]$ such that $[x/y] \in YY$ and $[x/y] \notin X$. Now $[x/y] = [a/b]\ [c/d]$ where $[a/b] \in Y$ and $[c/d] \in Y$. Choose the larger of $[a/b]$ and $[c/d]$. Suppose it is $[a/b]$. Then $[x/y] \leq [a/b]\ [a/b] \in X$. Thus, $[x/y] \in X$ and this contradicts that $[x/y] \notin X$. Hence YY is not greater than X.

Suppose $YY < X$. By 3.36 choose $[x/y]^*$ such that $YY < [x/y]^* < X$. Now $[x/y]^* = [a/b]^*\ [c/d]^*$ where $[a/b]^* \geq Y$ and $[c/d]^* \geq Y$. Let $[a/b]^*$ denote the lesser of $[a/b]^*$ and $[c/d]^*$. Then $[a/b]^* \geq Y$ which implies $[a/b]^*\ [a/b]^* \geq X$. Hence $[x/y] \in X$ and $[x/y] \notin X$ which is impossible. Thus, YY cannot be $<$ X. Hence, $YY = X$.

Theorem 3.38. $[a/b]^*\ [c/d]^* = [(ac)/(bd)]^*$

Proof. To show $[a/b]^*\ [c/d]^* \subset [(ac)/(bd)]^*$ let $[z/w] \in [a/b]^*\ [c/d]^*$. Then $[z/w] = [u/v]\ [r/s]$ where $[u/v] \in [a/b]^*$ and $[r/s] \in [c/d]^*$. Now, $[u/v] < [a/b]$ and $[r/s] < [c/d]$ which implies $[u/v]\ [r/s] < [a/b]\ [c/d] = [(ac)/(bd)]$. Hence, $[z/w] \in [(ac)/(bd)]^*$ and $[a/b]^*\ [c/d]^* \subset [(ac)/(bd)]^*$.

To show $[(ac)/(bd)]^* \subset [a/b]^*\ [c/d]^*$ let $[z/w] \in [(ac)/(bd)]^*$. Then $[z/w] < [(ac)/(bd)]$. Now there exists $[x/y]$ such that $[z/w] < [x/y] < [(ac)/(bd)] = [a/b]\ [c/d]$. Thus $[x/y]/[c/d] < [a/b]$. Also given $[z/w]$ and $[x/y]/[c/d]$ there exists $[u/v]$ such that $[z/w] = [u/v]\ ([x/y]/[c/d]) < [c/d] \cdot ([x/y]/[c/d]) = [c/d]$. Thus, $[u/v] < [c/d]$. Hence, $[z/w] = [u/v] \cdot ([x/y]/[c/d]) < [c/d]\ ([x/y]/[c/d]) < [c/d]\ [a/b] = [a/b]\ [c/d]$ where

$[u/v] \in [a/b]^*$ and $[x/y]/[c/d] \in [c/d]^*$. Thus $[z/w] \in [a/b]^* \; [c/d]^*$ and so $[(ac)/(bd)]^* \subset [a/b]^* \; [c/d]^*$. Hence $[a/b]^* \; [c/d]^* = [(ac)/(bd)]^*$.

Definition 3.39. Any cut which is not rational is called irrational.

Theorem 3.40. There exists an irrational number.

Proof. That the solution of $XX = 1'$ is irrational will be shown in what follows. We note that the existence of the solution is guaranteed by 3.37. Assume that X is rational; i.e., $X = [a/b]^*$. By Theorem 1.22 choose the representative of $[a/b]$ such that b is as small as possible. Since $1' = [a/b]^* \; [a/b]^* = [(aa)/(bb)]^* = XX$, $bb < 1'(bb) = aa = (1'b)b < (1'b)(1'b)$. Thus, $b < a < 1'b$. Set $a-b = u$. Then $b+u = a < 1'b = b+b$ which implies $u < b$. Set $b-u = t$. Then $aa + tt = (b+u)(b+u) + tt$

$$
\begin{aligned}
&= ((b+u)b + (b+u)u) + tt \\
&= ((bb + (ub + bu)) + uu) + tt \\
&= ((bb + 1'(ub)) + uu) + tt \\
&= ((bb + (1'u)(t+u)) + uu) + tt \\
&= (bb + 1'(uu)) + ((uu + 1'(ut)) + tt) \\
&= (bb + 1'(uu)) + (u+t)(u+t) \\
&= (bb + 1'(uu)) + bb \\
&= 1'(bb) + 1'(uu) \\
&= aa + 1'(uu)\,.
\end{aligned}
$$

Hence $tt = 1'(uu)$ which implies $(tt)\cdot 1 = 1'(uu)$ and so $[(tt)/(uu)]^* = 1'$. Thus $[t/u]^* \; [t/u]^* = 1'$. Hence $u > y$ since y was the smallest such natural number. But this contradicts $u < y$. Thus, $1'$ is irrational.

REAL NUMBERS

A new number, called a real number, defined in terms of ordered pairs of cuts is introduced in this section. It will be shown that the real numbers possess the commutative, associative, and distributive properties. Again it will be pointed out that a subset of the real numbers obey the axioms of the natural numbers under the appropriate definitions. The set of all real numbers will be denoted by R.

Definition 4.1. The ordered pair (X,Y) is equivalent to the ordered pair (Z,W) if and only if $X+W = Y+Z$. The relation will be denoted by $\sim$ and the ordered pair by $X-Y$.

Theorem 4.2. The relation is:

i) Reflexive: $X-Y \sim X-Y$

ii) Symmetric: if $X-Y \sim Z-W$, then $Z-W \sim X-Y$

iii) Transitive: if $X-Y \sim Z-W$ and $Z-W \sim T-U$, then $X-Y \sim T-U$

Proof. Trivial.

Hence, $\sim$ is an equivalence relation on the set of ordered pairs of cuts.

Definition 4.3. By a real number we mean the set of all ordered pairs equivalent to a given ordered pair. If (X,Y) is the given ordered pair, then the real number is denoted by $[X-Y]$.

Definition 4.4. Two real numbers, $[X-Y]$ and $[Z-W]$ are said to be equal if and only if $[X-Y] \subset [Z-W]$ and $[Z-W] \subset [X-Y]$. This will be denoted by $[X-Y] = [Z-W]$. Otherwise, $[X-Y] \neq [Z-W]$.

Theorem 4.5. $[X-Y] = [Z-W]$ if and only if $X-Y \sim Z-W$.

Proof. Assume $[X-Y] = [Z-W]$. Since $X-Y \in [X-Y]$, $X-Y \in [Z-W]$ by the hypothesis. Hence, $X-Y \sim Z-W$ by 4.3. To show the converse, assume

$X-Y \sim Z-W$. Let $T-U \in [X-Y]$. Then $T-U \sim X-Y$. Thus, by 4.2 (iii), $T-U \sim Z-W$ and so $T-U \in [Z-W]$. Hence, $[X-Y] \subset [Z-W]$. Similarly, $[Z-W] \subset [X-Y]$. Therefore, $[X-Y] = [Z-W]$ by 4.4.

Theorem 4.6. $[X-Y] = [Z-W]$ if and only if $X+W = Y+Z$.

Proof. Trivial.

Theorem 4.7. The relation = is:

i) Reflexive: $[X-Y] = [X-Y]$.

ii) Symmetric: if $[X-Y] = [Z-W]$, then $[Z-W] = [X-Y]$.

iii) Transitive: if $[X-Y] = [Z-W]$ and $[Z-W] = [T-U]$, then $[X-U] = [T-U]$

Proof. Trivial.

Hence, = is an equivalence relation on R.

Definition 4.8. By the sum of two real numbers, to be denoted by +, is meant the following: $[X-Y] + [Z-W] = [(X+Z) - (Y+W)]$.

Theorem 4.9. + is a binary operation on R.

Proof. It is obvious that the sum gives a real number. It must now be shown that the sum is well defined; that is, it doesn't depend on the particular ordered pairs of cuts used to name the real numbers. Symbolically, if $[X-Y] = [Z-W]$ and $[T-U] = [P-V]$, then we wish to show that $[X-Y] + [T-U] = [Z-W] + [P-V]$. Now, $X+W = Y+Z$ and $T+V = U+P$ by 4.6. So, $(X+W) + (T+V) = (Y+Z) + (U+P)$. Thus, $(X+T) + (W+V) = (Y+U) + (Z+P)$ which implies $(X+T) - (Y+U) = (Z+P) - (W+V)$ by 4.6 and so $[X-Y] + [T-U] = [Z-W] + [P-V]$ by 4.8. Hence, the theorem is shown.

Theorem 4.10. $[X-Y] + [Z-W] = [Z-W] + [X-Y]$.

Proof. $[X-Y] + [Z-W] = [(X+Z) - (Y+W)]$ by 4.8

$= [(Z+X) - (W+Y)]$

$= [Z-W] + [X-Y]$ by 4.8.

Theorem 4.11. $([X\text{-}Y] + [Z\text{-}W]) + [T\text{-}U] = [X\text{-}Y] + ([Z\text{-}W] + [T\text{-}U])$.

Proof. $([X\text{-}Y] + [Z\text{-}W]) + [T\text{-}U] = [X{+}Z - Y{+}W] + [T\text{-}U]$

$$= [((X+Z) + T) - ((Y+W) + U)]$$

$$= [(X + (Z+T)) - (y + (W+U))]$$

$$= [X\text{-}Y] + [(Z+T) - (W+U)]$$

$$= [X\text{-}Y] + ([Z\text{-}W] + [T\text{-}U])$$

Definition 4.12. By the product of two real numbers, to be denoted by $\cdot$, is meant the following: $[X\text{-}Y]\,[Z\text{-}W] = [(XZ + YW) - (YZ + XW)]$

Theorem 4.13. $\cdot$ is a binary operation on R.

Proof. It is obvious that the product is a real number. To show that the product gives an unique real number it must be shown that the particular given pair of cuts used to name the real number is arbitrary; that is, if $[X\text{-}Y] = [Z\text{-}W]$ and $[T\text{-}U] = [P\text{-}V]$, then we must show that $[X\text{-}Y]\,[T\text{-}U] = [Z\text{-}W]\,[P\text{-}V]$.

Proof. It is easy to show that $(XT + YU) + (WP + ZV) = (YT + XU) + (ZP + WV)$. Then $(XT + YU) - (YT + XU) = (ZP + WV) - (WP + ZV)$ Hence, $[X\text{-}Y]\,[T\text{-}U] = [Z\text{-}W]\,[P\text{-}V]$.

Theorem 4.14. $[X\text{-}Y]\,[Z\text{-}W] = [Z\text{-}W]\,[X\text{-}Y]$.

Proof. $[X\text{-}Y]\,[Z\text{-}W] = [(XZ + YW) - (YZ + XW)]$

$$= [(ZX + WY) - (ZY + WX)] \text{ by } 3.21$$

$$= [Z\text{-}W]\,[X\text{-}Y].$$

Hence, $[X\text{-}Y]\,[Z\text{-}W] = [Z\text{-}W]\,[X\text{-}Y]$.

Theorem 4.15. $([X\text{-}Y]\,[Z\text{-}W])\,[P\text{-}V] = [X\text{-}Y]\,([Z\text{-}W]\,[P\text{-}V])$

Proof. $([X\text{-}Y]\,[Z\text{-}W])\,[P\text{-}V] = [(XZ + YW) - (YZ + XW)]\,[P\text{-}V]$

$$= [((XZ + YW)P + (YZ + XW)V) - ((YZ + XW)P + (XZ + YW)V)]$$

$$= [(X(ZP + WV) + Y(WP + ZV)) - (Y(ZP + WV) + X(WP + ZV))]$$

$$= [X-Y]\ [(ZP + WV) - (WP + ZV)]$$

$$= [X-Y]\ [Z-W]\ P-V$$

Hence, $([X-Y][Z-W])[P-V] = [X-Y]([Z-W]\ [P-V])$

Theorem 4.16. $[X-Y]([Z-W] + [P-V]) = [X-Y]\ [Z-W] + [X-Y]\ [P-V]$.

Proof. $[X-Y]([Z-W] + [P-V]) = [X-Y]\ [(Z+P) - (W+V)]$

$$= [(X(Z+P) + Y(W+V)) - (Y(Z+P) + X(W+V))]$$

$$= [((XZ + YW) + (XP + YV)) - ((YZ + XW) + (YP + XV))]$$

$$= [((XZ + YW) - (YZ + XW)) + ((XP + YV) - (YP + XV))]$$

$$= [X-Y]\ [Z-W] + [X-Y]\ [P-V].$$

And so the theorem is proved.

Theorem 4.17. If $[X-Y] + [P-V] = [Z-W] + [P-V]$, then $[X-Y] = [Z-W]$.

Proof. $[X-Y] + [P-V] = [(X+P) - (Y+V)]$ and $[Z-W] + [P-V] = [(Z+P) - (W+V)]$. Thus, $(X+P) + (W+V) = (Y+V) + (Z+P)$. Hence, by 3.14 $X+W = Y+Z$ which implies $[X-Y] = [Z-W]$ by 4.6.

Theorem 4.18. $\exists /$ $[P-V]$ such that for every $[X-Y]$, $[X-Y] + [P-V] = [X-Y]$.

Proof. The uniqueness follows immediately from 4.17. Now $[P-V] = [Z-Z]$ is the solution since $[X-Y] + [P-V] = [X-Y] + [Z-Z]$

$$= [(X+Z) - (Y+Z)]$$

$= [X-Y]$ since $(X+Z) + Y = (Y+Z) + X$.

$[Z-Z]$ is called the additive identity on R.

Corollary. $[Z-Z] + [X-Y] = [X-Y]$.

Theorem 4.19. For each $[X-Y]$ $\exists /$ $[P-V]$ such that $[X-Y]$ + $[P-V]$ = $[Z-Z]$.

Proof. The uniqueness is obvious from 4.17. Now, $[P-V]$ = $[Y-X]$ is the solution since $[X-Y]$ + $[P-V]$ = $[X-Y]$ + $[Y-X]$

$$= [(X+Y) - (Y+X)]$$

$$= [Z-Z] \text{ since } (X+Y) + Z = (Y+X) + Z$$

$[Y-X]$ is called the additive inverse of $[X-Y]$ and will be denoted by $-[X-Y]$.

Corollary. $-[X-Y] + [X-Y] = [Z-Z]$.

Theorem 4.20. For every $[X-Y]$, $[X-Y]\,[(Z+1)-Z] = [X-Y]$.

Proof. $[X-Y]\,[(Z+1)-Z] = [(X(Z+1) + YZ) - (Y(Z+1) + XZ)]$

$$= [X-Y] \text{ since } (X(Z+1) + YZ) + Y = (Y(Z+1) + XZ) + X$$

Corollary. $[(Z+1) - Z]\,[X-Y] = [X-Y]$.

Theorem 4.21. If $[X-Y]\,[P-V] = [X-Y]$ for every $[X-Y]$, then $[P-V] = [(Z+1) - Z]$.

Proof. Now $[P-V]\,[(Z+1) - Z] = [P-V]$ by 4.20.

Also, $[P-V]\,[(Z+1) - Z] = [(Z+1) - Z]\,[P-V]$ by 4.14

$$= [(Z+1) - Z] \text{ by hypothesis.}$$

Hence, $[P-V] = [(Z+1) - Z]$ by 4.7 (iii). $[(Z+1) - Z]$ will be called the multiplicative identity on R.

Theorem 4.22. For each $[X-Y]$ there exists $[P-V]$ such that $[X-Y]\,[P-V] = [(Z+1) - Z]$ if $[X-Y] \neq [Z-Z]$.

Proof. $[P-V] = [X/((XX + YY) - 1'(XY)) - Y/((XX + YY) - 1'(XY))]$

$$= [(XX + YY)/((XX + YY) - 1'(XY)) - (YX + XY)/((XX + YY) - 1'(XY))]$$

$$= [(Z+1) - Z] \text{ since } ((XX + YY)/((XX + YY) - 1'(XY))) + Z =$$

$$(1'(XY)/((XX + YY) - 1'(XY))) + (Z+1)$$

We note that it can be shown that $(XX + YY) - 1'(XY)$ is a cut. Thus, the theorem is shown.

Corollary. $[P-V]\,[X-Y] = [(Z+1) - Z]$.

Hereafter, real numbers will be denoted by upper case letters such as A,B,C.... $[Z-Z]$ will be denoted by 0 and $[(Z+1)-Z]$ will be denoted by 1.

Theorem 4.23. $A\cdot 0 = 0$ for every A.

Proof. $A\cdot 0 = A\cdot(0+0)$

$= A\cdot 0 + A\cdot 0.$

Thus, $A\cdot 0 = 0$ by 4.18.

Corollary. $0\cdot A = 0$

Theorem 4.24. $A\cdot B = 0$ if and only if $A=0$ or $B=0$.

Proof. If $A=0$, then $A\cdot B = 0\cdot B = 0$ by 4.23 corollary. If $B=0$, then $A\cdot 0 = 0$ by 4.23.

Assume $A\cdot B = 0$ and $A\neq 0$. Then there exists C such that $CA = 1$ by 4.22 corollary. Hence, $C(AB) = (CA)B$ by 4.15.

$= 1\cdot B$

$= B$ by 4.20 corollary.

Also, $C(AB) = C\cdot 0$

$= 0$ by 4.23.

Hence, $B=0$. Similarly if $B\neq 0$, $A=0$.

Theorem 4.25. $(-A)\,B = -(AB)$

Proof. $AB + (-A)\,B = \big(A + (-A)\big)\,B$

$= 0\cdot B$

$= 0.$

Hence, $(-A)\,B = -(AB)$

Corollary $A(-B) = -(AB)$.

Theorem 4.26. $(-A)(-B) = AB$

Proof. $(-A)(-B) = (-A)(-B) + 0$

$= (-A)(-B) + (-AB + AB)$

$= (-A)(-B) + \big((-A)B + AB\big)$ by 4.25.

$= \big((-A)(-B) + (-A)B\big) + AB$

$= (-A)(-B+B) + AB$ by 4.16

$= (-A)\cdot 0 + AB$

$= -(A\cdot 0) + AB$

$= 0 + AB$

$= AB$

Hence, $(-A)(-B) = AB$.

Theorem 4.27. If $AB = AC$ and $A \neq 0$ then $B=C$. Now, $AB + -(AB) = 0$. Also,

Proof. $AB + -(AB) = AB + A(-B)$

$= AC + A(-B)$

$= A\big(C + (-B)\big)$

Hence $A\big(C + (-B)\big) = 0$. $A \neq 0$, so $C + (-B) = 0$ by 4.24.

Now, $B = B+0$

$= B + \big(C + (-B)\big)$

$= \big(B + (-B)\big) + C$

$= 0 + C$

$= C$.

And so $B = C$ if $A \neq 0$.

Theorem 4.28. The $[P-V]$ in 4.22 is unique.

Proof. The proof follows directly from 4.27

$[P-V]$ is called the multiplicative inverse of $[X-Y]$ and will be denoted by $1/[X-Y]$.

Theorem 4.29. $-(-A) = A$

Proof.
$$
\begin{aligned}
-(-A) &= -(-A) + 0 \\
&= -(-A) + \big((-A) + A\big) \\
&= \big(-(-A) + (-A)\big) + A \\
&= 0 + A \\
&= A
\end{aligned}
$$

Theorem 4.30. $-(A+B) = -A + (-B)$

Proof. $(A+B) + \big(-(A+B)\big) = 0$

Also,
$$
\begin{aligned}
(A+B) + \big((-A) + (-B)\big) &= \Big(B + \big(A + (-A)\big)\Big) + (-B) \\
&= (B+0) + (-B) \\
&= B + (-B) \\
&= 0
\end{aligned}
$$

Hence, $-(A+B) = -A + (-B)$.

Theorem 4.31. Given any A and B $\exists/$C such that $A = B+C$.

Proof. The uniqueness is obvious. $C = -B+A$ is the solution since
$$
\begin{aligned}
B+C &= B + (-B+A) \\
&= \big(B + (-B)\big) + A \\
&= 0 + A \\
&= A.
\end{aligned}
$$

C is called the difference of A and B and is denoted by $A-B$.

Corollary, $A-B = A + (-B)$

Theorem 4.32. Given A,B $\exists/$C such that $A = B \cdot C$ if $B \neq 0$.

Proof. The uniqueness follows directly from 4.27.

To show a solution exists let $C = 1/B \cdot A$. We note that $1/B$ exists since $B \neq 0$. Then
$$
\begin{aligned}
B \cdot C &= B \cdot (1/B \cdot A) \\
&= (B \cdot 1/B) \cdot A
\end{aligned}
$$

$= 1 \cdot A$

$= A.$

Hence, BC = A. C is called the quotient of A over B and is denoted by A/B.

Corollary. $A/B = A \cdot 1/B = 1/B \cdot A$.

Theorem 4.33. $-(A-B) = B-A$.

Proof.
$$
\begin{aligned}
-(A-B) &= -(A + (-B)) \\
&= -A + (-(-B)) \\
&= -A + B \\
&= B + (-A) \\
&= B-A
\end{aligned}
$$

Theorem 4.34. $A(B-C) = AB - AC$

Proof.
$$
\begin{aligned}
A(B-C) &= A(B + (-C)) \\
&= AB + A(-C) \\
&= AB + (-(AC)) \\
&= AB - AC
\end{aligned}
$$

Definition 4.35. X-Y is called a positive number if X Y and a negative number if Y X.

Definition 4.36. $A > B$ if and only if A-B is a positive number.

Definition 4.37. $A < B$ if and only if $B > A$.

Theorem 4.38. One and only one of the following can occur: A=B or $A > B$ or $A < B$.

Proof. Let $A-B = [X-Y]$. Either X=Y or $X > Y$ or $X < Y$. If X=Y, then $A-B = [X-X] = 0$. Hence, A=B. If $X > Y$ then $A-B = [X-Y]$ where $X > Y$. And so by 4.36, $A > B$. If $X < Y$, then $Y > X$. Now $-(A-B) = -[X-Y]$ and so, $B-A = [Y-X]$ where $Y > X$. Hence by 4.36 $B > A$ which implies $A < B$ by 4.37. Thus, the theorem is proved.

Theorem 4.39. $A=B$ or $A>B$ or $A<B$ if and only if $A+C = B+C$ or $A+C > B+C$ or $A+C < B+C$ respectively.

Proof. If $A=B$, then obviously $A+C = B+C$. If $A > B$, then $A-B$ is a positive number by 4.36. Also

$$\begin{aligned} A-B &= A + (-B) \\ &= (A+0) + (-B) \\ &= \big(A + (C + (-C))\big) + (-B) \\ &= (A+C) + \big((-B) + (-C)\big) \\ &= (A+C) + \big(-(B+C)\big) \\ &= (A+C) - (B+C). \end{aligned}$$

Hence, $(A+C) - (B+C)$ is a positive number. Therefore, $A+C > B+C$ by 4.36. If $A < B$, then $B > A$ by 4.37. And by preceding part $B+C > A+C$ which implies $A+C < B+C$ by 4.37.

The converse follows immediately from the above proof and the fact that the three cases are mutually exclusive and exhaust all possibilities.

Theorem 4.40. A is a positive number or A is a negative number if and only if $A > 0$ or $A < 0$ respectively.

Proof. If A is a positive real number, let $A = A+0$. Then $A-0 = A$. Hence, $A > 0$.

If A is a negative number, let $A = [X-Y]$. Then $Y > X$ by 4.35. Now $-A = -[X-Y] = [Y-X]$ where $Y > X$. Hence, $-A = 0 + (-A) = 0 - A = [Y-X]$ where $Y > X$. And so $0 > A$ by 4.36 which implies $A < 0$ by 4.37.

As for the converse, if $A > 0$ then $A = A-0 = [X-Y]$ where $X > Y$. Hence, by 4.35, A is a positive number.

If $A < 0$, then $0 > A$. Hence $-A = 0 + (-A) = 0-A = [X-Y]$ where $X > Y$. Thus $-A = [X-Y]$ and $-(-A) = A = [Y-X]$ where $X > Y$. And so by 4.35 A is a negative number.

Theorem 4.41. If $A > 0$ or $A=0$ or $A < 0$, then $-A < 0$ or $-A=0$ or $-A > 0$ respectively.

Proof. If $A > 0$ then $A = [X-Y]$ where $X > Y$. Hence, $-A = [Y-X]$. And so by 4.40, $-A < 0$. If $A=0$ then obviously $-A=0$. If $A < 0$ then $A = [X-Y]$ where $Y > X$. Hence $-A = [Y-X]$ and so by 4.40, $-A > 0$.

The converse follows from the above proof and the fact that the three cases are mutually exclusive and exhaust all possibilities.

Theorem 4.42. $A > B$ or $A = B$ or $A < B$ if and only if $A-B > 0$ or $A-B = 0$ or $A-B < 0$ respectively.

Proof. Trivial.

Theorem 4.43. If $A > B$ and $B > C$, then $A > C$.

Proof. $B > C$ implies $B-C=D$ where $D > 0$.

Hence, $B=C+D$. Thus, $A > B$

$$= C+D.$$

Now, $A > C + D$ and so $A-C > D$ which implies $A-C > 0$ and so, $A > C$.

Theorem 4.44. If $A > 0$ and $C > 0$ or $A < 0$ and $C > 0$ then $AC > 0$ or $AC < 0$ respectively.

Proof. If $A > 0$ and $C > 0$ then $A = [X-Y]$ where $X > Y$ and $C= [Z-W]$ where $Z > W$. Hence, $Z-W$ exists and $X(Z-W) > Y(Z-W)$ which implies $XZ - XW > YZ - YW$ and so $XZ + YW > XW + YZ$. Hence $[(XZ + YW) - (XW + YZ)] > 0$. And so $AC > 0$.

If $A > 0$ and $C < 0$ then $-C > 0$ and $A(-C) = -(AC) > 0$. Hence, $AC < 0$.

Theorem 4.45. $A > B$ if and only if $AC > BC$ or $AC = BC$ or $AC < BC$ for $C > 0$ or $C=0$ or $C < 0$ respectively.

Proof. Since $A > B$ then $A-B > 0$.

If $C > 0$, $(A-B)C > 0$ by 4.44. Hence $AC-BC > 0$ which implies $AC > BC$.

If C=0 then (A-B)C = 0 . Thus AC - BC = 0 which implies AC = BC.

If C < 0 then (A-B)C < 0 by 4.44.

Hence AC-BC < 0 implies AC < BC.

The converse following from the above proof since the cases are mutually exclusive and exhaust all possibilities.

Theorem 4.46. If A > 0 and B > 0, then A+B > 0.

Proof. Let A = [X-Y] where X > Y and B = [Z-W] where Z > W. Thus, X+Z > Y+W. Now A+B = [(X+Z) - (Y+W)] . Since X+Z > Y+W, A+B > 0.

Definition 4.47.

$$A = \begin{cases} A \text{ if } A > 0 \\ 0 \text{ if } A = 0 \\ -A \text{ if } A < 0 \end{cases}$$

Theorem 4.48. $|A| \geq 0$.

Proof. If A > 0 then $|A|$ = A and so $|A| > 0$. If A=0 then $|A| = 0$. If A < 0, then $|A|$ = -A. By 4.41, -A > 0. Hence, $|A| \geq 0$. In any case $|A| \geq 0$.

Theorem 4.49. $|A| \geq A$.

Proof. If $A \geq 0$, then $|A|$ = A. If A < 0 then $|A| = -A$ and -A > 0 by 4.41. Hence, by 4.43, A < -A and so $|A| > A$. In any case, $|A| \geq A$.

Theorem 4.50. The set of all real numbers of the form [X-Y] where X > Y and X-Y is an integral cut which hereafter will be called integral real numbers satisfy the axioms of the natural numbers if the role of 1 is assigned to 1 and if [X-Y]' = [X'-Y]; i.e.,

Axiom 1.IV. If [X-Y] = [Z-W] , then [X'-Y] = [Z'-W] .

Axiom 2.IV. There exists an element of R, denoted by 1 such that [X'-Y] ≠ 1.

Axiom 3.IV. If $[X'-Y] = [Z'-W]$, then $[X-Y] = [Z-W]$.

Axiom 4.IV. Let $\bar{M}$ be the set of integral real numbers such that $1 \in \bar{M}$ and $[X'-Y] \in \bar{M}$ whenever $[X-Y] \in \bar{M}$. Then $\bar{M}$ contains all integral real numbers.

Proof. If $[X-Y] = [Z-W]$, then $X+W = Y+Z$. Hence, $(X+W)' = (Y+Z)'$ by Axiom 1.III. Thus, $X'+W = Y+Z'$ and so $[X'-Y] = [Z'-W]$ and the axiom is proved.

The existence of 1 is obvious. $[X'-Y] \neq 1$ for if it did then $X' + Z = Y + (Z+1)$. Thus, $X' = Y+1 = Y'$ and $X = Y$. If $X=Y$, then $[X-Y]$ is not an integral real number and so $[X'-Y]$ is undefined. Hence, $[X'-Y] \neq 1$.

If $[X'-Y] = [Z'-W]$, then $X' + W = Y + Z'$. Hence $(X+W)' = (Y+Z)'$ and $X+W = Y+Z$ by Axiom 3.III. Hence, $[X-Y] = [Z-W]$.

Let M^* be the set of all integral cuts for which $[X-Y] \in \bar{M}$ and $Z = X-Y$. Now, $1 \in M^*$ since $1 \in \bar{M}$. Also, $Z' \in M^*$ whenever $Z \in M^*$ since $[X'-Y] \in \bar{M}$ whenever $[X-Y] \in \bar{M}$. Hence, M^* contains all integral cuts and $\bar{M}$ contains all integral real numbers.

It can be shown that the set of integral real numbers is isomorphic to the set of integral cuts.

Theorem 4.5. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two nonempty classes of real numbers such that if C is any element of $\mathcal{C}_1$ and D is any element of $\mathcal{C}_2$, then $C < D$. Then there exists one and only one real number A such that every $B < A$ belongs to $\mathcal{C}_1$ and every $B > A$ belongs to $\mathcal{C}_2$.

Proof. A is unique for if $B < C$ and B and C satisfy the requirements then $(B+C)/(1+1)$ would belong to both $\mathcal{C}_1$ and $\mathcal{C}_2$ since $(1+1)B = B+B < B+C < C+C = (1+1)C$. Hence, $B < (B+C)/(1+1) < C$.

To prove that A exists, consider four cases as follows:

I. Suppose $\mathcal{C}_1$ contains a positive number. Consider the set $\mathcal{A} = \{[a/b] : [a/b] \in \mathcal{C}_1\}$ except the greatest positive rational number if one exists. It will be shown that $\mathcal{A}$ is a cut.

(1) Since $\mathcal{C}_1$ contains an element $\exists / [a/b]^*$ by 3.35 less than this element such that $[a/b]^*$ is not the greatest such element. Hence, $[a/b]^* \in \mathcal{C}_1$ and $[a/b] \in \mathcal{A}$.

Also, since $\mathcal{C}_2$ contains an element $\exists [c/d]^*$ by 3.35 greater than this element. Hence, $[c/d]^* \in \mathcal{C}_2$ and $[c/d]^* \notin \mathcal{A}$.

(2) If $\mathcal{C}_1$ contains no greatest element, then every $[a/b]^*$ is less than every $[c/d]^* \in \mathcal{C}_2$. Hence, $[a/b] < [c/d]$ where $[a/b] \in \mathcal{A}$ and $[c/d] \notin \mathcal{A}$.

If $\mathcal{C}_1$ contains a greatest element say $[x/y]^*$, then every $[a/b]^* \neq [x/y]^*$ such that $[a/b]^* \in \mathcal{C}_1$ is less than $[x/y]^*$. Hence, $[a/b] < [x/y]$ where $[a/b] \in \mathcal{A}$ and $[x/y] \notin \mathcal{A}$. Since $[x/y]^* \in \mathcal{C}_1$, $[x/y]^* < [z/w]^*$ where $[z/w]^* \in \mathcal{C}_2$. Thus $[x/y] < [z/w]$ and $[a/b] < [x/y]$ implies every element of the set is less than every element not in the set.

(3) If $\mathcal{C}_1$ has a greatest member say $[x/y]^*$, then if $[a/b]^*$ is any other element of $\mathcal{C}_1$ then $[a/b]^* < [x/y]^*$. By 3.36, there exists $[z/w]^*$ such that $[a/b]^* < [z/w]^* < [x/y]^*$. Thus $[z/w]^* \in \mathcal{C}_1$. Hence $[a/b] < [z/w]$ and $\mathcal{A}$ has no greatest element.

If $\mathcal{C}_1$ has no greatest element, then if $[a/b]^* \in \mathcal{C}_1$ there exists $[z/w]^* \in \mathcal{C}_1$ such that $[a/b]^* < [z/w]^*$ which implies $[a/b] < [z/w]$. Thus, $\mathcal{A}$ has no greatest element.

Hence, $\mathcal{A}$ is a cut. Since $\mathcal{A}$ is a real number denote it by A.

Now to show that A satisfies Theorem 4.51. Let H be any real number such that $H < A$. If $H > 0$, there exists $[a/b]^*$ such that $H < [a/b]^* < A$

by 3.36. Since $[a/b] \in A$, $[a/b]^* \in \mathcal{C}_1$. Hence, $H \in \mathcal{C}_1$.

If $H < 0$, then $H < A/(1+1) < A$. By 3.36 there exists $[a/b]^*$ such that $H < A/(1+1) < [a/b]^* < A$. Thus $[a/b] \in A$ and $[a/b]^* \in \mathcal{C}_1$. Hence, $H \in \mathcal{C}_1$.

Let H be any real number such that $H > A$. Then $\exists [a/b]^*$ such that $H > [a/b]^* > A$. Thus, $[a/b] \notin A$ by 3.35 and $[a/b]^* \in \mathcal{C}_2$. Hence, $H \in \mathcal{C}_2$.

And so the theorem is proved for Case I.

II. Suppose every positive number lies in $\mathcal{C}_2$ and $0 \in \mathcal{C}_1$. Then every negative number lies in $\mathcal{C}_1$ and 0 satisfies the requirements.

III. Suppose 0 lies in $\mathcal{C}_2$, and every negative number lies in $\mathcal{C}_1$. Then every positive number lies in $\mathcal{C}_2$ and 0 satisfies the requirements.

IV. Suppose there exists a negative number in the second class. Consider the following new division. If $H1, \in \mathcal{C}_1$, put $-H1$, in new $\mathcal{C}_2$. If $H_2 \in \mathcal{C}_2$, put $-H_2$ in new $\mathcal{C}_1$. The new division satisfies the conditions of the theorem for:

(1) Each class contains a member.

(2) Since $H_1 < H_2$, $-H_2 < -H_1$.

This new division comes under Case I for since there exists a negative number C in $\mathcal{C}_2$, -C is positive and is an element of the new $\mathcal{C}_1$. Thus, there exists D such that every $B < D$ lies in the new $\mathcal{C}_1$ and every $B > D$ lies in the new $\mathcal{C}_2$. Set $D = -A$. Then $B < D$ or $B > D$ implies $-B > A$ or $-B < A$ respectively. If B is an element of the new $\mathcal{C}_1$ or the new $\mathcal{C}_2$; then $-B \in \mathcal{C}_2$ or $-B \in \mathcal{C}_1$ respectively. Hence, the theorem is satisfied.

COMPLEX NUMBERS

The complex number will be defined in terms of the real numbers. The binary operations of addition and multiplication (again denoted by + and ·) will be defined on the set of complex numbers. The associative, commutative and distributive properties will be established for the complex numbers. The definitions of complex conjugate and absolute value will be given with the basic theorems of absolute value and complex conjugates proved. Finally, it will be pointed out that there exists a subset of the complex numbers which is isomorphic to the real numbers.

Definition 5.1. A complex number is an ordered pair of real numbers A,B, denoted by $[A,B]$.

Definition 5.2. Two complex numbers $[A,B]$, $[C,D]$ are equal; i.e., $[A,B] = [C,D]$ if and only if A = C and B = D. Otherwise, $[A,B] \neq [C,D]$.

Lower case Greek letters will stand for complex numbers.

Theorem 5.3. The relation = is:

i) Reflexive: $\alpha = \alpha$.

ii) Symmetric: If $\alpha = \beta$, then $\beta = \alpha$.

iii) Transitive: If $\alpha = \beta$ and $\beta = \gamma$, then $\alpha = \gamma$.

Proof. Trivial.

Hence, = is an equivalence relation on the complex numbers.

Definition 5.4. $\eta = [0,0]$.

Definition 5.5. $e = [1,0]$.

Definition 5.6. $i = [0,1]$.

Definition 5.7. If $\alpha = [A,B]$ and $\beta = [C,D]$, then $\alpha + \beta = [A+C, B+D]$.

Theorem 5.8. $\alpha + \beta = \beta + \alpha$.

Proof. Let $\alpha = [A,B]$ and $\beta = [C,D]$, then

$\alpha + \beta = [A+C,\ B+D]$ by 5.7

$= [C+A,\ D+B]$

$= [C,D] + [A,B]$ by 5.7

$= \beta + \alpha$.

Hence, $\alpha + \beta = \beta + \alpha$.

Theorem 5.9. $\alpha + \eta = \alpha$ for every α.

Proof. Let $\alpha = [A,B]$, then

$\alpha + \eta = [A+0,\ B+0]$

$= [A,B]$ by 4.18

$= \alpha$

Hence, $\alpha + \eta = \alpha$. η is called the additive identity for complex numbers.

Corollary. $\eta + \alpha = \alpha$.

Theorem 5.10. If $\alpha + \beta = \alpha$ for all α, then $\beta = \eta$.

Proof. Let $\beta = [E,F]$ and $\alpha = [A,B]$. Then,

$\alpha + \beta = [A+E,\ B+F]$ by 5.7.

$= [A,B]$ since $\alpha + \beta = \alpha$.

Hence, $A+E = A$ and $B+F = B$ by 5.2. Thus $E=0$ and $F=0$ and so $\beta = \eta$.

Theorem 5.11. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

Proof. Let $\alpha = [A,B]$, $\beta = [C,D]$ and $\gamma = [E,F]$.

Then $(\alpha + \beta) + \gamma = \big([A,B] + [C,D]\big) + [E,F]$

$= [A+C,\ B+D] + [E,F]$

$= [(A+C) + E,\ (B+D) + F]$

$= [A + (C+E),\ B + (D+F)]$ by 4.11

$= [A,B] + [C+E,\ D+F]$

$= [A,B] + \big([C,D] + [E,F]\big)$

$= \alpha + (\beta + \gamma)$.

Hence, $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$.

Theorem 5.12. Given α and $\beta \; \exists / \gamma$ such that $\alpha = \beta + \gamma$.

Proof. Let $\alpha = [A,B]$, $\beta = [C,D]$ and $\gamma = [E,F]$.

γ is unique for if $\delta = [G,H]$ is also a solution then $\beta + \gamma = \beta + \delta$ which implies C+E = C+G and D+F = D+H by 5.2 and so E=G and F=H by 4.39 corollary. Hence $\delta = \gamma$.

$\gamma = [A-C, B-D]$ is the solution since $\beta + \gamma = [C + (A-C), D + (B-D)]$

$= [A,B]$ by 4.31

$= \alpha$.

γ is called the difference of α and β and is denoted by $\alpha - \beta$.

Theorem 5.13. For every $\alpha \; \exists / \beta$ such that $\alpha + \beta = \eta$.

Proof. The uniqueness was shown in the first part of 5.12.

If $\alpha = [A,B]$ then $\beta = [-A, -B]$ is the solution

since $\alpha + \beta = [A,B] + [-A, -B]$

$= [A + (-A), B + (-B)]$

$= [0, 0]$ by 4.19

$= \eta$ by 5.4.

β is called the additive inverse of α and is denoted by $-\alpha$. Thus, if $\alpha = [A,B]$, $-\alpha = [-A, -B]$.

Corollary. $-\alpha + \alpha = \eta$.

Theorem 5.14. $-(-\alpha) = \alpha$.

Proof. If $\alpha = [A,B]$, then $-\alpha = [-A,-B]$. Hence $-(-\alpha) = [-(-A),-(-B)] = [A,B]$ by 4. 29. Thus, $-(-\alpha) = \alpha$.

Theorem 5.15. $\alpha - \beta = \alpha + (-\beta)$.

Proof. $\alpha - \beta = (\alpha - \beta) + \eta$ by 5.9

$= (\alpha - \beta) + (\beta + (-\beta))$ by 5.13

$= ((\alpha - \beta) + \beta) + (-\beta)$ by 5.11

$= \alpha + (-\beta)$ by 5.12.

Hence, $\alpha - \beta = \alpha + (-\beta)$.

Theorem 5.16. $-(\alpha + \beta) = -\alpha + (-\beta)$

Proof. $-\alpha + (-\beta) = (-\alpha + (-\beta)) + \eta$

$= (-\alpha + (-\beta)) + ((\alpha + \beta) + (-(\alpha + \beta)))$

$= ((-\alpha + (-\beta)) + (\alpha + \beta)) + (-(\alpha + \beta))$

$= ((-\alpha + (-\beta + \beta)) + \alpha) + (-(\alpha + \beta))$

by 5.11 and 5.8.

$= ((-\alpha + \eta) + \alpha) + (-(\alpha + \beta))$ by 5.13 corollary

$= (-\alpha + \alpha) + (-(\alpha + \beta))$ by 5.9.

$= \eta + (-(\alpha + \beta))$

$= -(\alpha + \beta)$.

Hence, $-\alpha + (-\beta) = -(\alpha + \beta)$.

Theorem 5.17. $-(\alpha - \beta) = \beta - \alpha$.

Proof. $-(\alpha - \beta) = -(\alpha + (-\beta))$ by 5.15

$= -\alpha + (-(-\beta))$ by 5.16

$= -\alpha + \beta$ by 5.14

$= \beta + (-\alpha)$ by 5.8

$= \beta - \alpha$ by 5.15.

Hence, $-(\alpha - \beta) = \beta - \alpha$.

Definition 5.18. If $\alpha = [A,B]$ and $\beta = [C,D]$, then $\alpha\beta = [AC - BD, AD = BC]$.

Theorem 5.19. $\alpha\beta = \beta\alpha$.

Proof. Let $\alpha = [A,B]$ and $\beta = [C,D]$, then $\alpha\beta$

$= [AC - BD, AD + BC]$ by 5.18

$= [CA - DB, DA + CB]$ by 4.14

$= [C,D][A,B]$ by 5.18

$= \beta\alpha$.

Hence, $\alpha\beta = \beta\alpha$.

Theorem 5.20. $\alpha\eta = \eta$ for every α.

Proof. Let $\alpha = [A,B]$ then $\alpha\eta = [A,B][0,0]$

$= [A0 - B0, A0 + B0]$

$= [0,0]$

$= \eta$.

Hence $\alpha\eta = \eta$.

Corollary. $\eta\alpha = \eta$ for every α.

Theorem 5.21. $\alpha\beta = \eta$ if and only if $\alpha = \eta$ or $\beta = \eta$.

Proof. If $\alpha = \eta$ then $\alpha\beta = \eta$ by 5.20 corollary. Similarly, if $\beta = \eta$ then $\alpha\beta = \eta$.

Let $\alpha\beta = \eta$ and $\alpha = [A,B]$ and $\beta = [C,D]$.

Then $\alpha\beta = [A,B][C,D] = [AC - BD, AD + BC] = [0,0]$.

Hence, $AC - BD = 0$ and $AD + BC = 0$ by 5.2.

Then $AC = BD$ and $AD = -(BC)$ by 4.42

And so, $(AC)(AD) = (BD)(-BC)$

$= -\big((BD)(BC)\big)$ by 4.25.

Hence, $(AA)(CD) + (BB)(CD) = 0$ and so, $(AA + BB)(CD) = 0$. Assume $\alpha \neq \eta$; i.e., $A \neq 0$ or $B \neq 0$. Now $AA + BB > 0$ if $A \neq 0$ or $B \neq 0$ since $AA > 0$ by 4.24 if $A \neq 0$. Thus, $CD = 0$ by 5.21 which implies $C=0$ or $D=0$, also by 5.21. If $C=0$, then $BD = 0$ and $AD = 0$. $\alpha \neq \eta$ implies $D=0$. Similarly, if $D=0$, then $C=0$. Thus if $\alpha \neq \eta$, then $\beta = \eta$. Similarly if $\beta \neq \eta$, then $\alpha = \eta$ and the theorem is proved.

Theorem 5.22. $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

Proof. Let $\alpha = [A,B]$, $\beta = [C,D]$ and $\gamma = [E,F]$.

Then $(\alpha\beta)\gamma = \left([A,B]\,[C,D]\right)[E,F]$

$= [AC - BD,\ AD + BC]\,[E,F]$

$= [(AC - BD)E - (AD + BC)F,\ (AC - BD)F + (AD + BC)E]$

$= [A(CE - DF) - B(CF + DE),\ A(CF + DE) + B(CE - DF)$

$= [A,B]\,[CE - DF,\ CF + DE]$

$= [A,B]\left([C,D]\ [E,F]\right)$

$= \alpha(\beta\gamma)$.

Hence, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

Theorem 5.23. $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$.

Proof. Let $\alpha = [A,B]$, $\beta = [C,D]$ and $\gamma = [E,F]$.

Then $\alpha(\beta+\gamma) = [A,B]\left([C,D] + [E,F]\right)$

$= [A,B]\,[C+E,\ D+F]$

$= [A(C+E) - B(D+F),\ A(D+F) + B(C+E)]$

$= [(AC - BD) + (AE - BF),\ (AD + BC) + (AF + BE)]$

$= [AC - BD,\ AD + BC] + [AE - BF,\ AF + BE]$

$= [A,B]\,[C,D] + [A,B]\,[E,F]$

$= \alpha\beta + \alpha\gamma$.

Hence, $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$.

Corollary. $(\beta+\gamma)\alpha = \beta\alpha + \gamma\alpha$.

Theorem 5.24. $-(\alpha\beta) = (-\alpha)\beta$.

Proof. $(-\alpha)\beta = (-\alpha)\beta + \eta$

$= (-\alpha)\beta + \left(\alpha\beta + \left(-(\alpha\beta)\right)\right)$

$= \left((-\alpha)\beta + \alpha\beta\right) + \left(-(\alpha\beta)\right)$

$= (-\alpha+\alpha)\beta + \left(-(\alpha\beta)\right)$ by 5.23 corollary.

$= \eta\beta + \left(-(\alpha\beta)\right)$

$= \eta + \left(-(\alpha\beta)\right)$

$= -(\alpha\beta)$.

Hence, $-(\alpha\beta) = (-\alpha)\beta$.

Corollary. $-(\alpha\beta) = \alpha(-\beta)$.

Theorem 5.25. $(-\alpha)(-\beta) = \alpha\beta$.

Proof. $(-\alpha)(-\beta) = (-\alpha)(-\beta) + \eta$

$= (-\alpha)(-\beta) + \big(-(\alpha\beta) + \alpha\beta\big)$

$= (-\alpha)(-\beta) + \big((-\alpha)\beta + \alpha\beta\big)$ by 5.24

$= \big((-\alpha)(-\beta) + (-\alpha)\beta\big) + \alpha\beta$ by 5.22

$= (-\alpha)(-\beta+\beta) + \alpha\beta$ by 5.23

$= -\alpha\eta + \alpha\beta$

$= \eta + \alpha\beta$

$= \alpha\beta$.

Hence, $(-\alpha)(-\beta) = \alpha\beta$.

Theorem 5.26. If $\alpha\beta = \alpha\gamma$ and $\alpha \neq \eta$, then $\beta = \gamma$.

Proof. $\alpha\beta + \big(-(\alpha\gamma)\big) = \alpha\gamma + \big(-(\alpha\gamma)\big) = \eta$

$\alpha\beta + \big(-(\alpha\gamma)\big) = \alpha\beta + \alpha(-\gamma)$ by 5.24 corollary

$= \alpha\big(\beta + (-\gamma)\big)$ by 5.23

Hence, $\alpha\big(\beta + (-\gamma)\big) = \eta$. Since $\alpha \neq \eta$, $\beta + (-\gamma) = \eta$ by 5.21.

Thus, $\beta = \beta + \eta$

$= \beta + (-\gamma + \gamma)$

$= \big(\beta + (-\gamma)\big) + \gamma$

$= \eta + \gamma$

$= \gamma$.

Hence, $\beta = \gamma$.

Theorem 5.27. $\alpha e = \alpha$.

Proof. Let $\alpha = [A,B]$, then $\alpha e = [A,B]\,[1,0]$

$= [A\cdot 1 - B0\ ,\ A0 + B\cdot 1]$

$= [A,B]$

$= \alpha$.

e is called the multiplicative identity for complex numbers.

Corollary. $e\alpha = \alpha$.

Theorem 5.28. If $\alpha\beta = \alpha$ for all α then $\beta = e$.

Proof. $\beta = e\beta$ by 5.27 corollary

$= e$ since $\alpha\beta = \alpha$.

Hence $\beta = e$

Theorem 5.29. Given $\alpha \neq \eta$, $\exists / \beta$ such that $\alpha\beta = e$.

Proof. The uniqueness is obvious. Let $\alpha = [A,B]$ and since $\alpha \neq \eta$, either $A \neq 0$ or $B \neq 0$. Assume $A \neq 0$. Then if $A > 0$, $AA > A0 = 0$ by 4.44. If $A < 0$, then $AA > A0 = 0$ by 4.45. Thus, $AA > 0$ if $A \neq 0$. Hence $AA = BB > 0$. Then $\beta = [A/(AA + BB)\ ,\ -B/(AA + BB)]$ is the solution since

$\alpha\beta = [A,B][A/(AA + BB)\ ,\ -B/(AA + BB)]$

$= [A(A/(AA + BB))\ -B\ (-B/(AA + BB))\ ,\ A\ (-B/(AA + BB)) + B\ (A/(AA + BB))]$

$= (AA)\ (1/(AA + BB)) - B(-B)(1/(AA + BB)),\ (A\ (-B))\ 1/(AA + BB) + (BA)$

$1/(AA + BB)]$

$= [\ (AA + BB)\ \ 1/(AA + BB)\ ,\ (\ -(AB) + AB)\ \ 1/(AA + BB)]$

$= [1,\ 0]$

$= e$.

β is called the multiplicative inverse of α and is written as e/α .

Corollary. $(e/\alpha)\alpha = e$.

Theorem 5.30. Given α and β, $\exists / \gamma$ such that $\alpha = \beta\gamma$ if $\beta \neq \eta$.

Proof. The uniqueness is obvious. $\gamma = \alpha(e/\beta)$ is the solution since $\beta\gamma = \beta\ (\alpha(e/\beta))$

$= \beta((e/\beta)\alpha)$

$= (\beta(e/\beta))\alpha$

$= e\alpha$

$= \alpha$.

γ is called the quotient of α and β and is denoted by α/β .

Corollary. $\alpha/\beta = \alpha(e/\beta) = (e/\beta)\alpha$.

Definition 5.31. If $\alpha = [A, B]$, then $\bar{\alpha} = [A, -B]$ is called the complex conjugate of α .

Theorem 5.32. $\bar{\bar{\alpha}} = \alpha$.

Proof. Let $\alpha = [A,B]$, then $\bar{\alpha} = [A, -B]$ by 5.31. Hence $\bar{\bar{\alpha}}$

$= [A, -(-B)]$

$= [A, B]$ by 4.29.

$= \alpha$.

And so $\bar{\bar{\alpha}} = \alpha$.

Theorem 5.33. $\bar{\alpha} = \eta$ if and only if $\alpha = \eta$.

Proof. If $\alpha = \eta$ then if $\alpha = [A, B]$, A=0 and B=0. But B=0 implies -B=0 by 4.41. Then $\bar{\alpha} = [A, -B] = [0, 0] = \eta$.

If $\bar{\alpha} = \eta$ then A=0 and -B=0 which implies A=0 and B=0. Hence, $\alpha = \eta$.

Theorem 5.34. $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$.

Proof. Let $\alpha = [A,B]$, $\beta = [C,D]$, then $\alpha + \beta = [A+C, B+D]$.

Thus, $\overline{\alpha + \beta} = [A+C, -(B+D)]$ by 5.31

$= [A+C, -B + (-D)]$ by 4.30.

$= [A,-B] + [C, -D]$

$= \bar{\alpha} + \bar{\beta}$ by 5.31.

Hence, $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$.

Theorem 5.35. $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$.

Proof. Let $\alpha = [A,B]$ and $\beta = [C,D]$, then $\alpha\beta = [AC - BD, AD + BC]$.

Also $\overline{\alpha\beta} = [AC - BD, -(AD + BC)]$

$= [AC -(-B(-D)) , A(-D) + (-B) D]$

$= [A,-B][C,-D]$

$= \bar{\alpha}\ \bar{\beta}$.

Hence, $\overline{\alpha\beta} = \bar{\alpha}\,\bar{\beta}$.

Definition 5.36. If $A > 0$ the symbol $\sqrt{A}$ means the positive real number B of the equation $BB = A$ (see 3.37).

Definition 5.37. $\sqrt{0} = 0$.

Definition 5.38. $|[A,B]| = \sqrt{AA + BB}$.

Theorem 5.39. $|\alpha| > 0$ for $\alpha \neq \eta$ and $|\alpha| = 0$ for $\alpha = \eta$.

Proof. Let $\alpha = [A,B]$, then if $\alpha \neq \eta$, $|\alpha| = \sqrt{AA + BB}$ where $AA + BB > 0$. Hence $|\alpha| > 0$ by 5.36. If $\alpha = \eta$ then $|\alpha| = \sqrt{00 + 00} = \sqrt{0} = 0$ by 5.37.

Theorem 5.40. $|[A,B]| \geq |A|$ and $|[A,B]| \geq |B|$.

Proof. Suppose the hypothesis is false: i.e., $|[A,B]| < |A|$. Then $\sqrt{AA + BB} < |A|$. If $A=0$ then $|A| = 0$ and $\sqrt{AA + BB} < 0$ which contradicts 5.36 if $B \neq 0$ since $BB > 0$ or 5.37 if $B=0$.

If $A \neq 0$ then $|A| \neq 0$ and $AA + BB > 0$. By 3.37 $\sqrt{AA + BB}\ \sqrt{AA + BB} < |A|\ |A|$. If $A < 0$, $|A| = -A$ and so $|A|\,|A| = (-A)(-A) = AA$. If $A > 0$, $|A| = A$ and $|A|\,|A| = AA$. Hence, $|A|\,|A| = AA$. Thus, $AA + BB < AA = AA + 0$. And so, $BB < 0$ by 4.39 corollary. But $BB \geq 0$ and thus we have a contradiction. Hence, $|[A,B]| \geq |A|$. Similarly $|[A,B]| \geq |B|$.

Theorem 5.41. If $A \geq 0$ and $B \geq 0$ and if $[A,0][A,0] = [B,0][B,0]$ then $A=B$.

Proof. $[A,0][A,0] = [AA - 00, A0 + 0A]$

$= [AA, 0]$

$= [BB, 0]$ since $[A,0][A,0] = [B,0][B,0]$.

Hence $AA = BB$. Now, $A=B$ or $A < B$ or $A > B$. Suppose $A < B$ then $B \neq 0$. And so, $AA \leq AB < BB$ by 4.45and 4.24. Hence, $AA < BB$. If $A>B$, then $A \neq 0$ and so $AA > AB \geq BD$ by 4.45. Hence $AA > BB$. Therefore, $A=B$.

Theorem 5.42. $[|\alpha|, 0][|\alpha|, 0] = \alpha\bar{\alpha}$.

Proof. Let $\alpha = [A,B]$ then $[|\alpha|,0][|\alpha|,0] = [|\alpha|\,|\alpha|,0] = [AA + BB,0]$ $= [AA - (-(BB)), -(AB) + AB] = [AA - B(-B), A(-B) + BA] = [A,B][A,-B] = \alpha\bar{\alpha}$. Hence, $[|\alpha|,0][|\alpha|,0] = \alpha\bar{\alpha}$.

Theorem 5.43. $|\alpha\beta| = |\alpha|\,|\beta|$.

Proof. $[|\alpha\beta|,0][|\alpha\beta|,0] = (\alpha\beta)\overline{\alpha\beta}$ by 5.42

$= (\alpha\beta)(\bar{\alpha}\bar{\beta})$ by 5.34

$= (\alpha\bar{\alpha})(\beta\bar{\beta})$

$= ([|\alpha|,0][|\alpha|,0])([|\beta|,0][|\beta|,0])$

$= [|\alpha|\,|\alpha|,0][|\beta|\,|\beta|,0]$

$= [(|\alpha|\,|\alpha|)(|\beta|\,|\beta|),0]$

$= [|\alpha|\,|\beta|,0][|\alpha|\,|\beta|,0]$

Hence, $|\alpha\beta| = |\alpha|\,|\beta|$ by 5.39.

Theorem 5.44. $|\alpha/\beta| = |\alpha|/|\beta|$ if $\beta \neq \eta$.

Proof. If $\beta \neq \eta$, then $|\beta| \neq 0$ by 5.39. Now $\beta(\alpha/\beta) = \alpha$ by 5.30. Hence by 5.43,

$|\beta(\alpha/\beta)| = |\beta|\,|\alpha/\beta| = |\alpha|$. Since $|\beta| \neq 0, |\alpha/\beta| = |\alpha|/|\beta|$.

Theorem 5.45. If $\alpha + \beta = e$, then $|\alpha| + |\beta| \geq 1$.

Proof. Let $\alpha = [A,B]$ and $\beta = [C,D]$ then $|\alpha| \geq |A|$ and $|\beta| \geq |C|$ by 5.39. Since $|A| \geq A$ and $|C| \geq C$ by 4.49, $|\alpha| + |\beta| \geq A+C$. By the hypothesis, $A+C = 1$. Hence, $|\alpha| + |\beta| \geq 1$.

Theorem 5.46. $|\alpha + \beta| \leq |\alpha| + |\beta|$.

Proof. If $\alpha + \beta = \eta$ then $|\alpha + \beta| = 0$. Thus $|\alpha + \beta| \leq |\alpha| + |\beta|$.

If $\alpha + \beta \neq \eta$, then $|\alpha + \beta| > 0$. Hence $\alpha/(\alpha+\beta) + \beta/(\alpha+\beta)$

$= \alpha(e/\alpha+\beta) + \beta(e/(\alpha+\beta))$

$= (\alpha/\beta)(e/(\alpha+\beta))$

$= e$.

Hence, by 5.45. $|\alpha/(\alpha+\beta)| + |\beta/(\alpha+\beta)| \geq 1$.

Therefore, $|\alpha| + |\beta| = |\alpha + \beta| \; 1|\alpha| \, 1|\alpha+\beta| + |\alpha + \beta| \; 1 \; |\beta| \, 1/|\alpha+\beta|$

$$= |\alpha + \beta|\left(|\alpha/(\alpha+\beta)| + |\beta \; 1 \; (\alpha + \beta)|\right) \quad 5.43$$

$$\geq |\alpha + \beta| \cdot 1$$

$$= |\alpha + \beta| \; .$$

Hence, $|\alpha + \beta| \leq |\alpha| + |\beta|$.

Theorem 5.47. The complex numbers of the form [A,0] where A is an integral real number satisfy the axioms of the natural numbers if the role of 1 is assigned to [1,0] and if [A,0]' = [A',0] ; i.e.,

Axiom 1.V. If [A,0] = [B,0] then [A',0] = [B',0] .

Axiom 2.V. There exists a complex number [1,0] such that [A',0] $\neq$ [1,0]

Axiom 3.V. If [A',0] = [B',0] , then [A,0] = [B,0]

Axiom 4.V. Let [M] = {[A,0] :X is an integral real number} which has the following properties:

a) [1,0] $\in$ [M]

and b) if [A,0] $\in$ [M] , then [A,0] ' $\in$ [M] .

Then [M] contains all complex numbers of the form [A,0] where A is an integral real number.

Proof. Since [A,0] = [B,0] , A=B and so A'=B' by Axiom 1.IV. Thus, [A',0] = [B',0] by 5.2.

That 1 exists is obvious. Suppose [A',0] = [1,0] then A' = 1 by 5.2. But this contradicts Axiom 2.IV. Hence, [A',0] $\neq$ [1,0] .

Since [A',0] = [B',0] , A'=B' and so by Axiom 3.IV, A=B. Hence, [A,0 = B,0] .

Let M be the set of all A for which [A,0] $\in$ [M]. Then 1 $\in$ M since [1,0] $\in$ [M]. Also A' $\in$ M wherever A $\in$ M since if [A,0] $\in$ [M] so is [A,0 ']. Thus M contains all integral real numbers and hence [M] contains all complex numbers of the form [A,0] where A in an integral real number.

Moreover, if by definition $[A,0] > [B,0]$ if and only if $A > B$ and $[A,0] < [B,0]$ if and only if $[B,0] > [A,0]$, it can be shown that the subset of complex numbers, $\{[A,0]: A \in R\}$ is ismorphic to R relative to the corresponding operations of addition and multiplication.

In the following, A will stand for $[A,0]$ and will be called a real number.

Theorem 5.47. $ii = -1$.

Proof.
$$ii = [0,1]\,[0,1]$$
$$= [00 - 1\,1,\ 01 + 10]$$
$$= [-1,0]$$
$$= -1.$$

Hence, $ii = -1$.

Theorem 5.49. The complex number $[A,B]$ may be written uniquely in the form $A + Bi$ where A and B are real numbers.

Proof.
$$[A,B] = [A,0] + [0,B]$$
$$= [A,0] + [B0 - 01,\ B1 + 00]$$
$$= [A,0] + [B0][01]$$
$$= A + Bi.$$

Hence, $[A,B] = A + Bi$

LITERATURE CITED

Landau, Edmund Georg Hermann, 1871. Foundations of analysis. Chelsea Publishing Co., New York. (Translated by F. Steinhardt 1951.)