

VII INTEGER AND RATIONAL NUMBERS

Natural Numbers

Definition The **natural** or **counting** numbers are the elements of ω .

We use the blackboard bold face letter \mathbb{N} to represent the set of natural numbers. As the definition indicates they are synonymous with the ordinal number ω .

We note here that when the natural or counting numbers are developed via the Peano postulates, the set of natural numbers begins with 1 and do not include the number 0. The Whole numbers, indicated by \mathbb{W} , are considered to be the set of numbers that are the union of the natural numbers and $\{0\}$. However in the set theoretic development of numbers it is much more convenient to consider the natural numbers as the ordinal number ω , and not specify any particular set as being whole numbers. (The Peano postulates can be found in most elementary number theory texts, and also in *Naive Set Theory* by Paul R. Halmos.)

Integers

The next set of numbers we develop we shall call **Integer Numbers** and we will indicate this set by the bold face letter \mathbb{Z} (From the German word for counting, zahlen). For the purpose of brevity the integer numbers are referred to as **integers**. The rationale for the development of this set is that we may wish to answer questions such as: What number added to 2 is

0? This can be expressed symbolically by $x + 2 = 0$. We realize of course that $\{x \in \mathbb{N} \mid x + 2 = 0\} = \emptyset$, thus the question has a vacant answer in the natural numbers. We extend the natural numbers to a larger set in which this question and other questions like it have non-vacuous answers.

We define an equivalence relation on the cartesian product of the natural numbers with themselves, i.e., $\mathbb{N} \times \mathbb{N}$, by

$$(a, b) \equiv (c, d) \Leftrightarrow a + d = b + c.$$

The rationale for this definition is that each ordered pair represents a difference. Using our previous (to the study of set theory) concept of subtraction we see

$$a + d = b + c \Leftrightarrow a - b = c - d.$$

We leave it to the reader to verify that this relation is an equivalence relation. Also the reader should note and verify that this relation is **not** an equivalence relation for $\alpha \times \alpha$ where $\alpha > \omega$.

Definition The **integers** are the collection of equivalence classes of $\mathbb{N} \times \mathbb{N}$ with respect to the equivalence relation

$$(a, b) \equiv (c, d) \text{ if } a + d = b + c.$$

We will indicate the equivalence class of (a, b) by $[a, b]$, that is

$$[a, b] = \{(x, y) \mid (x, y) \equiv (a, b)\}.$$

We now wish to define an order and an arithmetic for the integers. First we need a pair of lemmas.

Lemma 7.1 $a + n = b + n \Rightarrow a = b \forall n \in \mathbb{N}$.

Proof Let $A = \{n \in \mathbb{N} \mid a + n = b + n \Rightarrow a = b \forall a, b \in \mathbb{N}\}$ and let $k \in \mathbb{N}$. If $k \geq 2$, then $S(k) = \{0, 1, 2, \dots, k-1\} \subset A$. Thus $a + 1 = b + 1 \Rightarrow a = b$, and $a + k - 1 = b + k - 1 \Rightarrow a = b$, for all $a, b \in \mathbb{N}$. We now assume $a + k = b + k$, which implies $a + k - 1 + 1 = b + k - 1 + 1$, which implies $a + k - 1 = b + k - 1$, which implies $a = b$. For $k = 1$ we have $a + 1 = b + 1 \Rightarrow a = b$ by Theorem 2.8. For $k = 0$, we have $a + 0 = a$ and $b + 0 = b$, thus $a + 0 = b + 0 \Rightarrow a = b$. All three cases imply $k \in A$. Thus by transfinite induction we have the desired result. ■

Lemma 7.2 $a + n < b + n \Rightarrow a < b \forall n \in \mathbb{N}$.

Proof: The proof is identical to the proof of the previous lemma by replacing “=” with “<”, except possibly the case $k = 1$. For the case $k = 1$, $a + 1 < b + 1 \Rightarrow a \cup \{a\} \subset b \cup \{b\}$. If $a \not\subset b$, then there exists $x \in a$ such that $x \notin b$. Since $x \in b \cup \{b\}$ we must have $x = b$. But either $a \in b$ or $a = b$, which contradicts the axiom of regularity. We thus conclude $a \subseteq b$. If $a = b$ we also have the obvious contradiction to the axiom of regularity, thus $a \subset b \Rightarrow a < b$. ■

There is a natural order that may be defined on the integers.

Definition $[a, b] < [c, d]$ iff $a + d < b + c$.

Since $[a, b]$ and $[c, d]$ represent equivalence classes, and the numbers a, b, c, d are specific values we must verify that the definition is valid regardless of what pair is chosen to represent each equivalence class. That is, we must show that the ordering is **well defined**.

Theorem 7.3 The ordering of the integers is well defined.

Proof Let $[a, b] < [c, d]$, $[a, b] = [x, y]$, and $[c, d] = [z, w]$. We have

$$\begin{aligned} & a + d < b + c, \quad a + y = b + x, \quad \text{and} \quad c + w = d + z \\ \Rightarrow & a + d + x + w < b + c + x + w = a + d + y + z \\ \Rightarrow & x + w < y + z \\ \Rightarrow & [x, y] < [z, w]. \quad \blacksquare \end{aligned}$$

We define addition and multiplication of integers as follows

$$\begin{aligned} [a, b] + [c, d] &= [a + c, b + d] \\ [a, b] \cdot [c, d] &= [ac + bd, ad + bc]. \end{aligned}$$

We now demonstrate that these operations are well defined.

Theorem 7.4 Addition and multiplication of integers are well defined.

Proof Let $(a, b) \equiv (x, y)$, and $(c, d) \equiv (z, w)$. We thus have

$$\begin{aligned} & a + c + y + w = b + d + x + z \\ \Rightarrow & (a + c, b + d) \equiv (x + z, y + w) \\ \Rightarrow & [a, b] + [c, d] = [x, y] + [z, w]. \end{aligned}$$

Hence addition is well defined.

For multiplication we have

$$\begin{aligned}
 & a + y = b + x \text{ and } c + w = d + z \\
 \Rightarrow & \quad ac + cy = bc + cx, \quad bd + dx = ad + dy, \\
 & \quad xw + cx = dx + xz \text{ and } yz + dy = cy + yw \\
 \Rightarrow & \quad ac + bd + xw + yz + cy + dx + cx + dy = \\
 & \quad ad + bc + xz + yw + cy + dx + cx + dy \\
 \Rightarrow & \quad ac + bd + xw + yz = ad + bc + xz + yw \\
 \Rightarrow & \quad (ac + bd, ad + bc) \equiv (xz + yw, xw + yz) \\
 \Rightarrow & \quad [a, b] \cdot [c, d] = [x, y] \cdot [z, w].
 \end{aligned}$$

Hence multiplication is well defined. ■

We must now develop the usual properties of the integers.

Theorem 7.5 If $a, b, c, d \in \mathbb{Z}$ with $c \neq 0$ and $d > 0$, then

i. $a = b \Leftrightarrow a + c = b + c.$

ii. $a = b \Leftrightarrow ac = bc.$

iii. $a < b \Leftrightarrow a + c < b + c.$

iv. $a < b \Leftrightarrow ad < bd.$

Proof Let $a = [a_1, a_2]$, $b = [b_1, b_2]$, $c = [c_1, c_2]$, $d = [d_1, d_2] > 0 \Rightarrow d_1 > d_2.$

i.

$$\begin{aligned}
a = b &\Leftrightarrow [a_1, a_2] = [b_1, b_2] \\
&\Leftrightarrow a_1 + b_2 = a_2 + b_1 \\
&\Leftrightarrow a_1 + b_2 + c_1 + c_2 = a_2 + b_1 + c_1 + c_2 \\
&\Leftrightarrow [a_1 + c_1, a_2 + c_2] = [b_1 + c_1, b_2 + c_2] \\
&\Leftrightarrow [a_1, a_2] + [c_1, c_2] = [b_1, b_2] + [c_1, c_2] \\
&\Leftrightarrow a + c = b + c
\end{aligned}$$

ii.

$$\begin{aligned}
a = b &\Leftrightarrow [a_1, a_2] = [b_1, b_2] \\
&\Leftrightarrow a_1 + b_2 = a_2 + b_1 \\
&\Leftrightarrow a_1c_1 + b_2c_1 = a_2c_1 + b_1c_1 \ \& \ a_1c_2 + b_2c_2 = a_2c_2 + b_1c_2 \\
&\Leftrightarrow a_1c_1 + b_2c_1 + a_2c_2 + b_1c_2 = a_1c_2 + b_2c_2 + a_2c_1 + b_1c_1 \\
&\Leftrightarrow (a_1c_1 + a_2c_2, a_1c_2 + a_2c_1) = (b_1c_1 + b_2c_2, b_1c_2 + b_2c_1) \\
&\Leftrightarrow ac = bc
\end{aligned}$$

iii.

$$\begin{aligned}
a < b &\Leftrightarrow [a_1, a_2] < [b_1, b_2] \\
&\Leftrightarrow a_1 + b_2 < a_2 + b_1 \\
&\Leftrightarrow a_1 + b_2 + c_1 + c_2 < a_2 + b_1 + c_1 + c_2 \\
&\Leftrightarrow [a_1 + c_1, a_2 + c_2] < [b_1 + c_1, b_2 + c_2] \\
&\Leftrightarrow [a_1, a_2] + [c_1, c_2] < [b_1, b_2] + [c_1, c_2] \\
&\Leftrightarrow a + c < b + c
\end{aligned}$$

iv.

$$\begin{aligned}
a < b & \Leftrightarrow [a_1, a_2] < [b_1, b_2] \\
& \Leftrightarrow a_1 + b_2 < a_2 + b_1 \\
& \Leftrightarrow a_1d_1 + b_2d_1 < a_2d_1 + b_1d_1 \ \& \ a_1d_2 + b_2d_2 < a_2d_2 + b_1d_2 \\
\text{also} \quad & a_1d_2 + b_2d_2 < a_1d_1 + b_2d_1 \ \& \ a_2d_2 + b_1d_2 < a_2d_1 + b_1d_1 \\
\text{since} & d_2 < d_1 \\
& \Leftrightarrow a_1d_1 + b_2d_1 + a_2d_2 + b_1d_2 < a_1d_2 + b_2d_2 + a_2d_1 + b_1d_1 \\
& \Leftrightarrow (a_1d_1 + a_2d_2, a_1d_2 + a_2d_1) < (b_1d_1 + b_2d_2, b_1d_2 + b_2d_1) \\
& \Leftrightarrow ad < bd
\end{aligned}$$

■

Definition An **injection** of a set a into a set b is a bijection from a to a subset of b . We will use the symbol \hookrightarrow to indicate that a map is an injection.

There is a natural injection, J , from \mathbb{N} to \mathbb{Z} defined by

$$J : x \hookrightarrow [x, 0].$$

When there exists an injection from one set to another that preserves order and arithmetic properties, we say the first set is **embedded** into the second. It is easy to verify that the natural injection is an embedding.

Lemma 7.6 If $[a, b]$ is an integer, then there exists a natural number c , such that $[a, b] = [c, 0]$, or $[a, b] = [0, c]$.

Proof By trichotomy, either $a > b$, $a = b$, or $a < b$. If $a > b$ let c be such that $b + c = a$, thus $[a, b] = [c, 0]$. If $a = b$ let $c = 0$ (recall for us that 0

is a natural number), thus $[a, b] = [0, 0] = [c, 0]$. If $a < b$ let c be such that $a + c = b$, thus $[a, b] = [0, c]$. ■

When $a + c = b$, and $a, b, c \in \mathbb{N}$, we express c as $b - a$.

It is convenient to represent an equivalence class by one of its elements. When a choice function is defined to choose from each of the equivalence classes a representative element, that element is known as the **canonical** representative.

For the integers we define our choice function to be

$$\phi([a, b]) = \begin{cases} (a - b, 0) & \text{if } a \geq b \\ (0, b - a) & \text{if } b > a \end{cases}$$

Thus every integer can be represented by $[a, 0]$ or $[0, a]$. When the numbers are understood to be integers we will use a to represent $[a, 0]$ and $-a$ to represent $[0, a]$. As an exercise the reader may wish to show that $a > 0$, and $-a < 0$, that is $[a, 0] > [0, 0]$, and $[0, a] < [0, 0]$.

Definition The set of integers strictly greater than 0 is called the **Positive Integers** and are denoted by \mathbb{Z}^+ . Those integers strictly less than 0 are called the **Negative Integers** and are denoted by \mathbb{Z}^- .

An Integral Domain

We leave it the reader to verify the following properties for \mathbb{Z} .

1. $a + b \in \mathbb{Z} \forall a, b \in \mathbb{Z}$.
2. $ab \in \mathbb{Z} \forall a, b \in \mathbb{Z}$.

3. $(a + b) + c = a + (b + c) \forall a, b, c \in \mathbb{Z}$.
4. $(ab)c = a(bc) \forall a, b, c \in \mathbb{Z}$.
5. $a + b = b + a \forall a, b \in \mathbb{Z}$.
6. $ab = ba \forall a, b \in \mathbb{Z}$.
7. $a(b + c) = ab + ac \forall a, b, c \in \mathbb{Z}$.
8. $\exists e \in \mathbb{Z}$ such that $a + e = e + a = a \forall a \in \mathbb{Z}$
9. $\exists u \in \mathbb{Z}$ such that $au = ua = a \forall a \in \mathbb{Z}$
10. $\forall a \in \mathbb{Z} \exists (-a) \in \mathbb{Z}$ such that $a + (-a) = (-a) + a = 0$
- 11*. If $ab = 0$, then either $a = 0$, or $b = 0$.

Properties 1 and 2 are called the closure properties, for addition and multiplication respectively, properties 3 and 4 are the associative properties, 5 and 6 are the commutative properties. Property 7 is the distributive property, we say multiplication distributes over addition. In properties 8 and 9 e and u are called the identities (again additive identity and multiplicative identity respectively). The $-a$ in property 10 is called the additive inverse, or opposite. We say that a number a is a zero divisor if $ab = 0$, but neither a nor b equal 0 (of course b is also a zero divisor). Property 11* is called the “no zero divisors” property.

Definition Any set with two binary operations satisfying these 11 properties is called an **Integral Domain**.

Rational Numbers

Another question we may wish to answer is: Two times what number is 1? This can be represented symbolically by $2x = 1$. Again this question has a vacant answer in the set of integers.

We extend the integers to the set of rational numbers by defining the appropriate equivalence relation on the cartesian product of the integers with themselves. We use the bold face letter \mathbb{Q} to represent rational numbers. The letter \mathbb{Q} comes from the term quotient, i.e., the rational numbers are a collection of quotients.

Definition The **rational numbers** are the collection of equivalence classes of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ with respect to the equivalence relation

$$(x, y) \equiv (z, w) \Leftrightarrow xw = yz.$$

From the above comment we can see the rationale for this definition. Using our previous notion of quotients we see $xw = yz \Leftrightarrow \frac{x}{y} = \frac{z}{w}$ provided $y, w \neq 0$. The reader should again verify that the relation is an equivalence relation.

If we let $a, b \in \mathbb{Z}$ such that $a \geq 0$ and $b > 0$, then the reader should verify that $[-a, -b] \equiv [a, b]$ and $[a, -b] \equiv [-a, b]$. Thus we may (and shall) assume for any rational number $[a, b]$ that $b > 0$. Let d be the least element of $\{y | (x, y) \in [a, b] \text{ and } b > 0\}$. We then let the unique element $(c, d) \in [a, b]$ be the canonical representative of the rational number $[a, b]$.

We again have the natural order defined on the rational numbers given by

$$[x, y] < [z, w] \text{ iff } xw < yz.$$

Theorem 7.7 The ordering of rational numbers is well defined.

Proof Let $[x, y] = [a, b]$, $[z, w] = [c, d]$, and $[x, y] < [z, w]$ with $b, d, y, w > 0$. We thus have

$$\begin{aligned} ay = bx, \quad dz = cw \text{ and } xw < yz \\ \Rightarrow bdx y w^2 < bdy^2 z w \Rightarrow ady^2 w^2 < bcy^2 w^2 \Rightarrow ad < bc \Rightarrow [a, b] < [c, d]. \end{aligned}$$

Hence the ordering is well defined. ■

We define addition and multiplication as follows,

$$\begin{aligned} [x, y] + [z, w] &= [xw + zy, yw] \\ [x, y] \cdot [z, w] &= [xz, yw]. \end{aligned}$$

Theorem 7.8 Addition and multiplication of rational numbers are well defined.

Proof Let $[x, y] = [a, b]$ and $[z, w] = [c, d]$.

For addition we have

$$\begin{aligned} ay = bx \text{ and } dz = cy \\ \Rightarrow aydw = bxdw \text{ and } bydz = bycw \\ \Rightarrow bdxw + bdyz = adyw + bcyw \\ \Rightarrow [xw + yz, yw] = [ad + bc, bd]. \end{aligned}$$

Hence addition is well defined.

For multiplication we have

$$\begin{aligned} ay = bx \text{ and } dz = cy \\ \Rightarrow acyw = bdxz \\ \Rightarrow [ac, bd] = [xz, yw]. \end{aligned}$$

Hence multiplication is well defined. ■

Just as there is a natural embedding of the natural numbers into the integers, there is the natural embedding of the integers into the rational numbers given by the injection,

$$J : x \mapsto [x, 1].$$

It is easy to verify that this injection is an embedding.

A Field

We leave it the reader to verify the following properties of \mathbb{Q} .

1. $a + b \in \mathbb{Q} \forall a, b \in \mathbb{Q}$.
2. $ab \in \mathbb{Q} \forall a, b \in \mathbb{Q}$.
3. $(a + b) + c = a + (b + c) \forall a, b, c \in \mathbb{Q}$.
4. $(ab)c = a(bc) \forall a, b, c \in \mathbb{Q}$.
5. $a + b = b + a \forall a, b \in \mathbb{Q}$.
6. $ab = ba \forall a, b \in \mathbb{Q}$.
7. $a(b + c) = ab + ac \forall a, b, c \in \mathbb{Q}$.
8. $\exists e \in \mathbb{Q}$ such that $a + e = e + a = a \forall a \in \mathbb{Z}$
9. $\exists u \in \mathbb{Q}$ such that $au = ua = a \forall a \in \mathbb{Q}$
10. $\forall a \in \mathbb{Q} \exists (-a) \in \mathbb{Q}$ such that $a + (-a) = (-a) + a = 0$
11. $\forall a \in \mathbb{Q}, a \neq 0, \exists a^{-1}$ such that $aa^{-1} = a^{-1}a = 1$

The first 10 properties are identical to the properties of an Integral Domain. Property 11* is replaced by property 11 where a^{-1} is called the multiplicative inverse, or reciprocal.

Any set with two binary operations satisfying these 11 properties is called a **Field**.

Exercise Show that every field is an integral domain. That is to say, every field has no zero divisors.

Differences and Quotients

Definition The **difference** between integers or rational numbers a and b is $a + (-b)$, which is written $a - b$.

Definition The **quotient** of two rational numbers a and b is $a \cdot b^{-1}$, which is written $\frac{a}{b}$.

We can see that difference and quotient can be regarded as a binary operations, we also notice that neither operation is commutative nor associative.

Exercise For any two rational numbers $p < q$, show that $p < \frac{p+q}{2} < q$.

Exercise Show that

1. If p, q, r are rational numbers where $p \leq q$ and $r > 0$, then $pr \leq qr$.
2. If p, q, r are rational numbers where $p \leq q$ and $r < 0$, then $pr \geq qr$.
3. If p and q are positive rational numbers, then $\frac{p}{q} \geq 1 \Rightarrow \frac{q}{p} \leq 1$.

Mathematical Induction

The next theorem is a special case of transfinite induction, that is widely used in many situations. Before we state and prove the theorem we need two small lemmas that we present as exercises.

Exercise 1. Define the map $\phi : \mathbb{N} \rightarrow \mathbb{Z}^+$ by $\phi(a) = [a + 1, 0]$. Show that $\phi(a) + 1 = \phi(a + 1)$.

Exercise 2. Show that \mathbb{Z}^+ is order isomorphic to ω .

Theorem 7.9 *The Principle of Mathematical Induction* If $T \subseteq \mathbb{Z}^+$ such that the following conditions are true:

- i. $1 \in T$
- ii. if $k \in T$, then $k + 1 \in T$,

then $T = \mathbb{Z}^+$.

Proof Consider the order preserving bijection $\phi : \omega \rightarrow \mathbb{Z}^+$ defined by $\phi(a) = [a + 1, 0]$. Let $A = \phi^{-1}(T)$. Let $x \in \omega$ such that $S(x) \subset A$.

If $x = 0$, then $\phi(x) = 1 \in T \Rightarrow x \in A$. If $x \neq 0$, then

$$\begin{aligned}
 S(x) \subset A &\Rightarrow x - 1 \in A \\
 &\Rightarrow \phi(x - 1) \in T \\
 &\Rightarrow \phi(x - 1) + 1 \in T \\
 &\Rightarrow \phi(x) \in T \\
 &\Rightarrow x \in A.
 \end{aligned}$$

Thus by Transfinite Induction $A = \omega \Rightarrow T = \phi(A) = \phi(\omega) = \mathbb{Z}^+$. ■

The Cardinality of Integers and Rational Numbers

Theorem 7.10 Both the integers and the rational numbers are countable.

Proof By Theorem 4.4 we know that $\mathbb{N} \times \mathbb{N}$ is countable. there exists the natural embedding of \mathbb{Z} into $\mathbb{N} \times \mathbb{N}$ by identifying $[a, b]$ with its canonical representative $(a - b, 0)$ or $(0, b - a)$. Thus there exists a bijection from \mathbb{Z} to a subset of a countable set, hence \mathbb{Z} is countable. Again by Theorem 4.4 we know that $\mathbb{Z} \times \mathbb{Z}$ is countable, and there exists the natural embedding of \mathbb{Q} into $\mathbb{Z} \times \mathbb{Z}$ by identifying $[a, b]$ with its canonical representative, (c, d) where d is positive and minimal. Thus there exists a bijection from \mathbb{Q} to a subset of a countable set, hence \mathbb{Q} is countable. ■

Let \mathbb{Z}_* represent the image of the embedding of \mathbb{Z} into \mathbb{Q} . Also let \mathbb{Z}_*^+ and \mathbb{Z}_*^- represent respectively the images of the embeddings of the positive and negative integers into the rationals.

The Archimedian Property

Theorem 7.11 *Archimedian Property* $\forall r \in \mathbb{Q} \exists n \in \mathbb{Z}_*^+$ such that $r < n$.

Proof Let $r = [a, b]$, if $r \leq 1$, then $r < 2$ and we are done. If $r > 1$, then without loss of generality, both a , and b are positive integers, and

$$\begin{aligned} b(a + 1) &\geq a + 1 > a \\ \Rightarrow [a, b] &< [a + 1, 1] \in \mathbb{Z}_*^+. \quad \blacksquare \end{aligned}$$

Lemma For positive rational numbers r and s , if $r > s$, then $r^{-1} < s^{-1}$.

Proof First we note that if $r = [a, b]$, then $r^{-1} = [b, a]$, this is immediate by computing $[a, b] \cdot [b, a] = [ab, ab] = [1, 1]$. Now let $r = [a, b]$ and $s = [c, d]$.

$$\begin{aligned} [a, b] > [c, d] &\Leftrightarrow ad > bc \\ &\Leftrightarrow [d, c] > [b, a] \\ &\Leftrightarrow s^{-1} > r^{-1}. \quad \blacksquare \end{aligned}$$

For any integer, a , the product of a with itself b times, where b is a positive integer is denoted a^b .

Exercise Prove that for any positive integer, n , there exists an integer of the form 2^m for some positive integer m , such that $2^m > n$. (Hint: use induction).

Solution For $n = 1$, $1 < 2 = 2^1$. Now assume $n < 2^m$ for some m , then $n + 1 < 2^m + 1 < 2^m + 2^m = 2^{m+1}$.

Exercise Prove that for any positive rational number, q , there exists a rational number of the form 2^n , where $2^n > q$, and where n is the embedded image of a positive integer.

Solution Let $q = (a, b)$ where a and b are positive integers. We then have $(a, b) \leq (a, 1) < (2^n, 1)$ for some n .

The Division Algorithm

Theorem 7.12 *The division algorithm* If a and d are integers with $d > 0$, then there exist unique integers q and r such that $a = dq + r$ and $0 \leq r < d$.

Proof This result is a consequence of the well ordering property.

Let $S = \{x \in \mathbb{Z} \mid x = a - dn \ \forall n \in \mathbb{Z}\}$, and let $S' = \{x \in S \mid x \geq 0\}$, S' is thus

the embedded image of some subset of \mathbb{N} , and thus if it is non-empty it must have a least element.

If $a \geq 0$, then let $n = 0$, and thus $x = a - 0 = a \geq 0$. Thus $a \in S'$. If $a < 0$, then let $n = a$, thus $x = a - ad = a(1-d) \geq 0$. Thus $a - ad \in S'$. Thus $S' \neq \emptyset$. Since $S' \neq \emptyset$, and is embedded image of a subset of \mathbb{N} , S' has a least element. Let the least element be r . Thus we have $r = a - dq \leq s \forall s \in S'$ and $a = dq + r$ where $r \geq 0$.

We now must show $r < d$. We have $a - d(q+1) = a - dq - d = r - d$, thus $r - d \in S$. Since r is the least element in S' and $r - d < r$ we have $r - d < 0 \Rightarrow r < d$. We thus have $a = dq + r$ with $0 \leq r < d$.

Now we have to show that q and r are unique. Suppose $a = dq_1 + r_1$ and $a = dq_2 + r_2$ where $0 \leq r_1 < d$ and $0 \leq r_2 < d$. Without loss of generality we may assume $r_1 \leq r_2$. We thus have $0 \leq r_2 - r_1 < r_2 < d$. We note that $0 \leq r_2 - r_1 = a - dq_2 - a + dq_1 = d(q_1 - q_2)$. Thus $r_2 - r_1$ is a multiple of d and non-negative. We thus have $0 \leq r_2 - r_1 < d$ and $r_2 - r_1 = d(q_1 - q_2) \Rightarrow 0 \leq d(q_1 - q_2) < d \Rightarrow 0 \leq q_1 - q_2 < 1 \Rightarrow q_1 - q_2 = 0$. Thus $q_1 = q_2$, and thus $r_1 - r_2 = 0 \Rightarrow r_1 = r_2$. ■

Exercises

1. Verify that the relation $(a, b) \equiv (c, d) \Leftrightarrow a + d = b + c$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$, but **not** on $\alpha \times \alpha$ where $\alpha > \omega$.
2. Verify that the relation $(x, y) \equiv (z, w) \Leftrightarrow xw = yz$ is an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$

For any Integral Domain D show:

3. $a \cdot e = e \forall a \in D$ and where e is the additive identity.
4. $u \cdot (-u) = -u$, where u is the multiplicative identity.
5. $(-u) \cdot (-u) = u$, where u is the multiplicative identity.
6. If $a, z \in D$ and $a + z = a$, then show $z = e$.

Solution to 3: $a = a \cdot u = a \cdot (u + e) = a + a \cdot e \Rightarrow a \cdot e = e$.

7. If $v, a \in F$, where F is a field and $a \cdot v = a$, then show $v = u$.
8. Show that every Field is an Integral Domain.

Mathematical Induction is often used to prove certain identities. Exercise 9 and its solution exemplifies how this is done. Exercise 10 is left as practice.

9. Show that $\sum_{k=1}^n k = \frac{n(n+1)}{2} \forall n \in \mathbb{Z}^+$.

Solution to 9: Let $A = \left\{ n \mid \sum_{k=1}^n k = \frac{n(n+1)}{2} \right\}$

- i. $\sum_{k=1}^1 k = 1 = \frac{1(2)}{2}$ thus $1 \in A$.

ii. Assume $m \in A$, then

$$\sum_{k=1}^{m+1} k = m + 1 + \sum_{k=1}^m k = m + 1 + \frac{m(m+1)}{2} = \frac{(m+1)(m+2)}{2}.$$

Thus $m + 1 \in A$. Therefore by Mathematical Induction $A = \mathbb{N}$,

and

$$\sum_{k=1}^n k = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{Z}^+.$$

10. Show that $\sum_{k=1}^n 2k - 1 = n^2 \quad \forall n \in \mathbb{Z}^+.$