

## Axioms of the integers $\mathbb{Z}$ .

The word “integer” is our undefined term (sometimes referenced as the “primitive” term) for this section. The set  $\mathbb{Z}$  is the set of all integers (Axiom D3 implies that  $\mathbb{Z}$  has at least two elements, so I am grammatically correct in using the plural). The set  $\mathbb{Z}$  satisfies the following axioms.

The usual rules (axioms) of logic are to be used to prove theorems from these axioms. As needed these rules will be discussed and stated. As a first such, following are the properties of the equality symbol.

- i.) [Reflexive]  $x = x$  for all  $x$ .
- ii.) [Symmetric] If  $x = y$  then  $y = x$ .
- iii.) [Transitive] If  $x = y$  and  $y = z$  then  $x = z$ .
- iv.) [Uniqueness of function values] If  $f$  is a function and  $x = y$  then  $f(x) = f(y)$ .

Axioms about addition and multiplication: There exists two operations on the integers: addition denoted by “+” and multiplication denoted by “ $\cdot$ ”. [Strictly speaking “+” is a map from the cross product of the integers with itself into the integers with certain properties as defined by the axioms, and similarly for multiplication “ $\cdot$ ”.] Note that  $a \cdot b$  is usually written as  $ab$ . It is this functional definition and properties of the  $=$  symbol that yields the following (axioms) which will be needed for proofs and for which you may assume as part of our logic system.

If  $a = b$  and  $c = d$  then  $a + c = b + d$ .

If  $a = b$  and  $c = d$  then  $a \cdot c = b \cdot d$ .

[Observation: the symbols  $\wedge$  and  $\vee$  also satisfy these properties.]

### Axioms about addition.

A1. If  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z}$  then  $a + b \in \mathbb{Z}$ . [Closure.]

A2. If  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z}$  then  $a + b = b + a$ . [Commutativity.]

A3. If  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$  and  $c \in \mathbb{Z}$  then  $a + (b + c) = (a + b) + c$ . [Associativity.]

A4. There exists an element  $0 \in \mathbb{Z}$  so that if  $a \in \mathbb{Z}$  then  $a + 0 = a$ .  
[Additive Identity element.]

A5. If  $a \in \mathbb{Z}$  then there exists an element in  $\mathbb{Z}$  denoted by  $-a$  so that  $-a + a = 0$ . [Additive inverse.]

Definition:  $a - b$  means  $a + (-b)$ .

### **Axioms about multiplication.**

B1. If  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z}$  then  $a \cdot b \in \mathbb{Z}$ . [Closure.]

B2. If  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z}$  then  $a \cdot b = b \cdot a$ . [Commutativity.]

B3. If  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$  and  $c \in \mathbb{Z}$  then  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ . [Associativity.]

B4. There exists an element  $1 \in \mathbb{Z}$  so that if  $a \in \mathbb{Z}$  then  $a \cdot 1 = a$ .  
[Multiplicative Identity element.]

B5. If  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ ,  $c \in \mathbb{Z}$  with  $c \neq 0$  and  $ac = bc$  then  $a = b$ .  
[Cancellation rule.]

### **Axiom on the relationship between addition and multiplication.**

C1. If  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$  and  $c \in \mathbb{Z}$  then  $a \cdot (b + c) = a \cdot b + a \cdot c$ . [Distributive law.] (Note the assumption that the order of operation is to perform  $\cdot$  first then  $+$ . In other words  $ab + cd$  means  $(ab) + (cd)$ .)

### **Axioms on order.**

There exists an order relation " $<$ " so that:

D1. If each of  $a$  and  $b$  is an integer then exactly one of the following is true:

$$a < b, \quad a = b, \quad b < a.$$

D2. If each of  $a$ ,  $b$  and  $c$  is an integer  $a < b$  and  $b < c$ , then  $a < c$ .

D3.  $0 < 1$ .

D4. If each of  $a$ ,  $b$  and  $c$  is an integer and  $a < b$ , then  $a + c < b + c$ .

D5. If each of  $a$ ,  $b$  and  $c$  is an integer  $a < b$  and  $0 < c$ , then  $a \cdot c < b \cdot c$ .

Definition. The integer  $p$  is said to be positive if and only if  $0 < p$ ;  
 $\mathbb{N} = \{n \in \mathbb{Z} | 0 < n\}$ .

D6. If  $n$  is an integer then exactly one of the following is true [Trichotomy Law.]:

$$n \in \mathbb{N}, \quad n = 0, \quad -n \in \mathbb{N}.$$

Notation: The statement  $a > b$  means that  $b < a$ .

### Induction axiom.

E1. Suppose that  $S$  is a subset of  $\mathbb{N}$  containing 1 such that if  $n \in S$  then  $n + 1 \in S$ . Then  $S = \mathbb{N}$ .

An alternate, but equivalent, statement of the induction axiom is the following:

E1'. If  $S$  is a non-empty subset of  $\mathbb{N}$ , then  $S$  has a least element.

Strictly speaking, the positive integers  $\mathbb{N}$  is defined inductively as follows:

$$1 \in \mathbb{N} \tag{1}$$

$$\text{if } n \in \mathbb{N} \text{ then } n + 1 \in \mathbb{N} \tag{2}$$

and  $\mathbb{N}$  is the minimal set satisfying conditions (1) and (2) above.

Then axiom E1 tells us that anything satisfying conditions (1) and (2) is  $\mathbb{N}$ .