The Axioms of Arithmetic[1]

Let's play a game. Let R be a nonempty set. A **binary operation** is a function from $R \times R$ to R. That is a binary operation takes two elements from R and outputs a single element of R. We shall suppose that we have two binary operations on R. The first is called *addition*. Given a and b in R addition gives an element $a + b$ in R. The other is called *multiplication*. Given a and b in R multiplication gives $a \cdot b \in R$. We shall assume that these two operations obey the axioms listed below. The game is to prove facts about R based solely on these axioms.

Axioms: For all a, b and c in R the following hold.

a. $a + b = b + a$ (addition is commutative)

b. $a + (b + c) = (a + b) + c$ (addition is associative)

c. There is an element $z \in R$,
independent of a,
such that $z + a = a$ (an additive identity exists)

d. There is an $\bar{a} \in R$,
which depends on a,
such that $\bar{a} + a = z$ (additive inverses exist)

e. $a \cdot b = b \cdot a$ (multiplication is commutative)

f. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (multiplication is associative)

g. There is an element $u \in R$,
independent of a,
such that $u \cdot a = a$ (a multiplicative identity exists)

h. If a is not an additive identity,
there is an $\hat{a} \in R$,
which depends on a,
such that $\hat{a} \cdot a = u$ (multiplicative inverses exist)

i. $a \cdot (b + c) = a \cdot b + a \cdot c$ (multiplication distributes over addition)

Applications:

[1] ©Michael C. Sullivan, September 14, 2001

1. There is only one additive identity element in R. *Proof:* Suppose z_1 and z_2 are both additive identity elements. Then by (c) $z_1 + z_2 = z_2$ and $z_2 + z_1 = z_1$. But, by (a), $z_1 + z_2 = z_2 + z_1$. Thus, $z_1 = z_2$.

   We are now justified in saying that the "zero element" is unique and shall denote it by 0.

2. There is only one multiplicative identity element in R. *Proof:* **Problem 1**. The unique "unity element" shall be denoted by 1.

3. Additive inverses are unique. *Proof 1:* Let $a \in R$. Suppose $\bar{a}_1$ and $\bar{a}_2$ are additive inverses of a. Then $\bar{a}_1 = 0 + \bar{a}_1 = (\bar{a}_2 + a) + \bar{a}_1 = \bar{a}_2 + (a + \bar{a}_1) = \bar{a}_2 + (\bar{a}_1 + a) = \bar{a}_2 + 0 = \bar{a}_2$. The reader should check that each step used exactly one of the axioms. *Proof 2:* $a + \bar{a}_1 = 0 \Rightarrow \bar{a}_2 + (a + \bar{a}_1) = \bar{a}_2 + 0 \Rightarrow (\bar{a}_2 + a) + \bar{a}_1 = \bar{a}_2 \Rightarrow 0 + \bar{a}_1 = \bar{a}_2 \Rightarrow \bar{a}_1 = \bar{a}_2$. Note that we have used a basic property of all binary functions in adding $\bar{a}_2$ to both sides of an equation and have freely used more than one axiom per step.

4. Multiplicative inverses are unique. *Proof:* **Problem 2**.

5. Let $a \in R$. Then $a \cdot 0 = 0$. *Proof:* $a \cdot 0 = a \cdot 0 + 0 = a \cdot 0 + (a + \bar{a}) = (a \cdot 0 + a) + \bar{a} = (a \cdot 0 + a \cdot 1) + \bar{a} = a \cdot (0 + 1) + \bar{a} = a \cdot 1 + \bar{a} = a + \bar{a} = 0$. The reader should check each step to see which of the axioms are being applied.

6. Let $a \in R$. Then $\bar{\bar{a}} = a$. *Proof:* **Problem 3**. Hint: Start with $\bar{\bar{a}} = \bar{\bar{a}} + 0$.

7. Let $a \in R$. Then $\bar{a} = \bar{1} \cdot a$. *Proof:* Since additive inverses are unique we need only show that $a + \bar{1} \cdot a = 0$. $a + \bar{1} \cdot a = 1 \cdot a + \bar{1} \cdot a = a \cdot 1 + a \cdot \bar{1} = a \cdot (1 + \bar{1}) = a \cdot 0 = 0$. Notice the last step uses 5.

8. Let $a \in R - \{0\}$. Then $\hat{\hat{a}} = a$. *Proof:* **Problem 4**.

9. Let a and b be in R and suppose that $a \cdot b = 0$. Then either $a = 0$ or $b = 0$. *Proof:* **Problem 5**.

10. Let $a + c = b + c$. Then $a = b$. *Proof:* **Problem 6**.

11. **Problem 7**: Let $ac = bc$. Show that it need not follow that $a = b$.

If we let R be the real numbers $\mathbb{R}$ then the axioms apply to the normal addition and multiplication operations. It is customary to denote the additive inverse of a by $-a$ and its multiplicative inverse by a^{-1} or $1/a$, for $a \neq 0$.

Problem 8. Prove that $-1 \times -1 = 1$.

If we let R be rationals $\mathbb{Q}$, or the complex numbers $\mathbb{C}$, then the axioms still apply. This is clear for $\mathbb{Q}$. But for $\mathbb{C}$ it takes a bit of effort to show this. For the integers $\mathbb{Z}$ only axiom h fails to hold.

Problem 9. It is easy to check that $\mathbb{C}$ obeys axioms a through g and i. The only difficulty is axiom h. Let $a + ib \in \mathbb{C} - \{0\}$. Find $c + id \in \mathbb{C}$ such that $(a+ib)(c+id) = 1$, and thus establish axiom h. (It is to be understood that a, b, c and d are real numbers.)

Project 1. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Define addition and multiplication as follows. Let $a \oplus b$ be the remainder of $a + b$ divided by n and let $a \otimes b$ the remainder of $a \times b$ divided by n. For example, in $\mathbb{Z}_7$ we get $5 \oplus 5 = 3$, because $10 \div 7$ has remainder 3; and $4 \otimes 5 = 6$, because $20 \div 7$ has remainder 6. The set $\mathbb{Z}_n$ is called the *integers modulo* n and the operations are referred to as *modular arithmetic*.

(a) Show that $\mathbb{Z}_n$ satisfies axioms a through g and i.

(b) Show that $\mathbb{Z}_7$ satisfies axiom h but that $\mathbb{Z}_6$ does not.

(c) Study various $\mathbb{Z}_n$. Under what conditions does $\mathbb{Z}_n$ satisfy axiom h?