The Ring of Integers

Elementary number theory is largely about the **ring of integers**, denoted by the symbol $\mathbb{Z}$. The integers are an example of an algebraic structure called an **integral domain**. This means that $\mathbb{Z}$ satisfies the following axioms:

(a) $\mathbb{Z}$ has operations $+$ (addition) and $\cdot$ (multiplication). It is **closed** under these operations, in that if $m, n \in \mathbb{Z}$, then $m + n \in \mathbb{Z}$ and $m \cdot n \in \mathbb{Z}$.

(b) Addition is **associative**: If $m, n, p \in \mathbb{Z}$, then

$$m + (n + p) = (m + n) + p.$$

(c) There is an **additive identity** $0 \in \mathbb{Z}$: For all $n \in \mathbb{Z}$,

$$n + 0 = n \quad \text{and} \quad 0 + n = n.$$

(d) Every element has an **additive inverse**: If $n \in \mathbb{Z}$, there is an element $-n \in \mathbb{Z}$ such that

$$n + (-n) = 0 \quad \text{and} \quad (-n) + n = 0.$$

(e) Addition is **commutative**: If $m, n \in \mathbb{Z}$, then

$$m + n = n + m.$$

(f) Multiplication is **associative**: If $m, n, p \in \mathbb{Z}$, then

$$m \cdot (n \cdot p) = (m \cdot n) \cdot p.$$

(g) There is an **multiplicative identity** $1 \in \mathbb{Z}$: For all $n \in \mathbb{Z}$,

$$n \cdot 1 = n \quad \text{and} \quad 1 \cdot n = n.$$

(h) Multiplication is **commutative**: If $m, n \in \mathbb{Z}$, then

$$m \cdot n = n \cdot m.$$

(i) The **Distributive Laws** hold: If $m, n, p \in \mathbb{Z}$, then

$$m \cdot (n + p) = m \cdot n + m \cdot p \quad \text{and} \quad (m + n) \cdot p = m \cdot p + n \cdot p.$$

(j) There are **no zero divisors**: If $m, n \in \mathbb{Z}$ and $m \cdot n = 0$, then either $m = 0$ or $n = 0$.

Remarks.

(a) As usual, I'll often abbreviate $m \cdot n$ to mn.

(b) The last axiom is equivalent to the **Cancellation Property**: If $a, b, c \in \mathbb{Z}$, $a \neq 0$, and $ab = ac$, then $b = c$.

Here's the proof:

$$\begin{aligned} & abac \\ ab - ac &= 0 \\ a(b - c) &= 0 \end{aligned}$$

Since there are no zero divisors, either $a = 0$ or $b - c = 0$. Since $a \neq 0$ by assumption, I must have $b - c = 0$, so $b = c$.

Notice that I didn't *divide* both sides of the equation by a — I cancelled a from both sides. This shows that division and cancellation aren't "the same thing".

Example. If $n \in \mathbb{Z}$, prove that $0 \cdot n = 0$.

$$\begin{array}{rcll} 0 \cdot n & = & (0+0) \cdot n & \text{(Additive identity)} \\ & = & 0 \cdot n + 0 \cdot n & \text{(Distributive Law)} \end{array}$$

Adding $-(0 \cdot n)$ to both sides, I get

$$-(0 \cdot n) + 0 \cdot n = -(0 \cdot n) + (0 \cdot n + 0 \cdot n).$$

By associativity for addition,

$$-(0 \cdot n) + 0 \cdot n = (-(0 \cdot n) + 0 \cdot n) + 0 \cdot n.$$

Then using the fact that $-(0 \cdot n)$ and $0 \cdot n$ are additive inverses,

$$0 = 0 + 0 \cdot n.$$

Finally, 0 is the additive identity, so

$$0 = 0 \cdot n. \quad \square$$

Example. If $n \in \mathbb{Z}$, prove that $-n = (-1) \cdot n$.

In words, the equation says that the additive inverse of n (namely $-n$) is equal to $(-1) \cdot n$. What *is* the additive inverse of n? It is the number which gives 0 when added to n.

Therefore, I should add $(-1) \cdot n$ and see if I get 0:

$$\begin{array}{rcll} (-1) \cdot n + n & = & (-1) \cdot n + 1 \cdot n & \text{(Multiplicative identity)} \\ & = & (-1+1) \cdot n & \text{(Distributive Law)} \\ & = & 0 \cdot n & \text{(Additive inverse)} \\ & = & 0 & \text{(Preceding result)} \end{array}$$

By the discussion above, this proves that $-n = (-1) \cdot n$. $\square$

Example. Give an example of a set of objects with a "multiplication" which is not commutative.

If you have had linear algebra, you know that matrix multiplication is not commutative in general. For instance, considering 2×2 real matrices,

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad \text{but} \quad \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 0 & 0 \end{bmatrix}. \quad \square$$

The integers are **ordered** — there is a notion of greater than (or less than). Specifically, for $m, n \in \mathbb{Z}$, $m > n$ is defined to mean that $m - n$ is a **positive integer**: an element of the set $\{1, 2, 3, \ldots\}$.

Of course, $m < n$ is defined to mean $n > m$. $m \geq n$ and $m \leq n$ have the obvious meanings.

There are several order axioms:

(k) The positive integers are closed under addition and multiplication.

(l) (**Trichotomy**) If $n \in \mathbb{Z}$, either $n > 0$, $n < 0$, or $n = 0$.

Example. Prove that if $m > 0$ and $n < 0$, then $mn < 0$.

$n < 0$, so $0 - n = -n$ is a positive integer. $m > 0$ means $m = m - 0$ is a positive integer, so by closure $m \cdot (-n)$ is a positive integer.

By a property of integers (which you should try proving from the axioms), $m \cdot (-n) = -(mn)$. Thus, $-(mn)$ is a positive integer. So $0 - mn = -(mn)$ is a positive integer, which means that $0 > mn$. □

Well-Ordering Axiom. Every nonempty subset of the positive integers has a smallest element.

Your long experience with the integers makes this principle sound obvious. In fact, it is one of the deeper axioms for $\mathbb{Z}$. Some consequences include the **Division Algorithm** and the principle of **mathematical induction**.

Example. Prove that $\sqrt[3]{2}$ is not a rational number.

The proof will use the Well-Ordering Property.

I'll give a proof by contradiction. Suppose that $\sqrt[3]{2}$ is a rational number. In that case, I can write $\sqrt[3]{2} = \dfrac{a}{b}$, where a and b are positive integers.

Now

$$\sqrt[3]{2} = \frac{a}{b}, \quad \text{so} \quad b\sqrt[3]{2} = a, \quad \text{and} \quad 2b^3 = a^3.$$

(To complete the proof, I'm going to use some divisibility properties of the integers that I haven't proven yet. They're easy to understand and pretty plausible, so this shouldn't be a problem.)

The last equation shows that 2 divides a^3. This is only possible if 2 divides a, so $a = 2c$, for some positive integer c. Plugging this into $2b^3 = a^3$, I get

$$2b^3 = 8c^3, \quad \text{or} \quad b^3 = 4c^3.$$

Since 2 divides $4c^3$, it follows that 2 divides b^3. As before, this is only possible if 2 divides b, so $b = 2d$ for some positive integer d. Plugging this into $b^3 = 4c^3$, I get

$$8d^3 = 4c^3, \quad \text{or} \quad 2d^3 = c^3.$$

This equation has the same form as the equation $2b^3 = a^3$, so it's clear that I can continue this procedure indefinitely to get e such that $c = 2e$, f such that $d = 2f$, and so on.

However, since $a = 2c$, it follows that $a > c$; since $c = 2e$, I have $c > e$, so $a > c > e$. Thus, the numbers a, c, e, ... comprise a set of positive integers *with no smallest element*, since a given number in the list is always smaller than the one before it. This contradicts Well-Ordering.

Therefore, my assumption that $\sqrt[3]{2}$ is a rational number is wrong, and hence $\sqrt[3]{2}$ is not rational. □
