Axioms for the integers

Axioms 1 – 10 on handout

- Every fact you know (or don't) about integers follows from these axioms.

- For the moment, let's imagine that we only know these axioms.

What can we deduce?

For example, it's not even clear that $\mathbb{N}$ is equal to $\{1, 2, 3, \ldots\}$.

Lemma: For any $a, b, c \in \mathbb{Z}$, if $a+b = a+c$, then $b = c$. [Additive Cancellation]

Proof: Suppose $a, b, c \in \mathbb{Z}$ and $a+b = a+c$. Then

$$
\begin{aligned}
b &= 0 + b && \text{(Identity)} \\
&= (-a + a) + b && \text{(Additive inverses)} \\
&= -a + (a+b) && \text{(Associativity)} \\
&= -a + (a+c) && \text{(Given)} \\
&= (-a + a) + c && \text{(Associativity)} \\
&= 0 + c && \text{(Additive inverses)} \\
&= c. && \text{(Identity)}
\end{aligned}
$$

Note: Typically use associativity + commutativity without comment.

Ex: Additive inverses are <u>unique</u>.

If $a, b \in \mathbb{Z}$ with $a+b = 0$, then since $a + (-a) = 0$ also, we have $a+b = a+(-a)$. Thus $b = -a$ by cancellation. ✓

Other basic facts:

Lemma: For any $a \in \mathbb{Z}$, $a \cdot 0 = 0$.

Proof: Let $a \in \mathbb{Z}$. Then

$$a \cdot 0 = a \cdot (0 + 0) \quad \text{(Identity)}$$
$$= a \cdot 0 + a \cdot 0. \quad \text{(Distributive Law)}$$

Also, $a \cdot 0 = a \cdot 0 + 0$ by the Identity axiom, so

$$a \cdot 0 + a \cdot 0 = a \cdot 0 + 0.$$

By Cancellation, we get $a \cdot 0 = 0$. ☺

Lemma: For any $a \in \mathbb{Z}$, $-(-a) = a$. (HW8)

Lemma: For any $a, b \in \mathbb{Z}$, if $a \cdot b = 0$, then $a = 0$ or $b = 0$.

Idea: Prove the contrapositive: if $a \neq 0$ and $b \neq 0$, then $a \cdot b \neq 0$.

Consider cases.

Thm: For any $a, b, c \in \mathbb{Z}$ with $a \neq 0$,
if $a \cdot b = a \cdot c$, then $b = c$.

[Multiplicative Cancellation]

Proof: Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$, and suppose

$$a \cdot b = a \cdot c.$$

Then
$$a \cdot b - a \cdot c = 0$$
$$a(b-c) = 0$$

So $a = 0$ or $b - c = 0$ by the previous lemma. But $a \neq 0$, so $b - c = 0$. That is, $b = c$. ∎

Note: We haven't defined division, and we didn't need it.

Order Properties of $\mathbb{Z}$

Def: For $a, b \in \mathbb{Z}$, $a < b$ means $b - a \in \mathbb{N}$.

- $a \leq b$ means $a < b$ or $a = b$.
- $a > b$ means $b < a$.

Ex: $0 < a \iff a - 0 \in \mathbb{N} \iff a \in \mathbb{N}$.

Lemma: For any $a, b \in \mathbb{Z}$, exactly one of the following is true:

(i) $a < b$
(ii) $a = b$
(iii) $a > b$

Proof: Exercise.

In other words, $\mathbb{Z}$ is <u>linearly ordered</u> by $<$.