Homework 2: Props 1.12-14, 1.24, 1.25(i), 1.26

> **Prop. 1.12**
> $(x \in \mathbb{Z})\ (m \in \mathbb{Z})\ m + x = m \Rightarrow x = 0$

Proof.
Let $x, m \in \mathbb{Z}$.

- $(m + x) + (-m) = m + (-m)$, by adding the additive inverse (-m) to both sides
- $(m + (-m)) + x = m + (-m)$, by Axiom 1.1(ii)
- $0 + x = 0$, by Axiom 1.4.
- Finally, $x = 0$, by Prop. 1.7.

> **Prop. 1.13.**
> Let $x \in \mathbb{Z}$. $(\exists m \in \mathbb{Z})$ *such that* $m + x = m \Rightarrow x = 0$.

Proof.
Let $x \in \mathbb{Z}$, $m = 0$.
We know $(0 \in \mathbb{Z})$ by Axiom 1.2.

- $0 + x = 0$, by substitution
- Finally, $x = 0$, by Prop. 1.7.

> **Prop. 1.14**
> $(\forall m \in \mathbb{Z})\ m \cdot 0 = 0 = 0 \cdot m$

Proof.
Let $m \in \mathbb{Z}$.

- $m = m$
- $m \cdot 0 = m \cdot 0$, by multiplying both sides by 0

We know $0 + 0 = 0$, from Prop. 1.7.

- $m \cdot (0 + 0) = m \cdot 0$, by substitution

- $m \cdot 0 + m \cdot 0 = m \cdot 0$, by Axiom 1.1(iii)

We know $(m \cdot 0) \in \mathbb{Z}$, due to the closure property of binary operations.
We know the additive inverse $-(m \cdot 0) \in \mathbb{Z}$, by Axiom 1.4.

- $(m \cdot 0 + m \cdot 0) + (-(m \cdot 0)) = m \cdot 0 + (-(m \cdot 0))$, by adding $-(m \cdot 0)$ to both sides
- $m \cdot 0 + (m \cdot 0 + (-(m \cdot 0))) = m \cdot 0 + (-(m \cdot 0))$, by Axiom 1.1(ii)
- $m \cdot 0 + 0 = 0$, by Axiom 1.4
- Finally, $m \cdot 0 = 0$ by Axiom 1.2.

$m \cdot 0 = 0 \cdot m$, by Axiom 1.1(iv)
$\therefore m \cdot 0 = 0 = 0 \cdot m$ by transitivity.

> **Prop. 1.24**
> $(x \in \mathbb{Z})\ x \cdot x = x \Rightarrow x = 1 \vee x = 0$

Proof.
Assume $x \cdot x = x$, $x \neq 1$ and $x \neq 0$.
We know $m \cdot 1 = m$, by Axiom 1.3. Then by substitution, $x = x \cdot 1$.

- $x \cdot x = x = x \cdot 1$, AKA $x \cdot x = x \cdot 1$ by transitivity
- $x = 1$, by Axiom 1.5 since it is assumed $x \neq 0$

Contradiction, we have proved that $x = 1$ but have previously assumed $x \neq 1$.
$\therefore (x = 1) \vee (x = 0)$ holds true.

> **Prop. 1.25 (i)**
> $\forall m, n \in \mathbb{Z},\ -(m+n) = (-m) + (-n)$

Proof.
Let $m, n \in \mathbb{Z}$.
$-(m+n)$ is an additive inverse of $(m+n)$, by Axiom 1.4.
Prove $(-m) + (-n)$ is an additive inverse of $(m+n)$.

- $(m+n) + ((-m) + (-n))$
- $((m+n) + (-m)) + (-n)$, by associativity of addition
- $((m + (-m)) + n) + (-n)$, by associativity of addition
- $(m + (-m)) + (n + (-n))$, by associativity of addition

- $0+0$, by the axiom of additive inverses.
- Finally, we reduce to 0, by prop. 1.7.

$\therefore\ (-m)+(-n)$ is an additive inverse of $(m+n)$.
$(m+n)+((-m)+(-n))=0$ and $(m+n)+(-(m+n))=0$ are true.
By prop. 1.9, $(-m)+(-n)=-(m+n)$.

> **Prop. 1.26**
> $(m,n \in \mathbb{Z})\ mn=0 \Rightarrow m=0 \vee n=0$

Proof.
Let $m,n \in \mathbb{Z}$.
Assume $mn=0$, $m \neq 0$ and $n \neq 0$.
We know $m \cdot 0 = 0$, by Prop. 1.14.

- $mn=0=m \cdot 0$, AKA $mn = m \cdot 0$ by transitivity
- $n=0$, by Axiom 1.5 since it is assumed $m \neq 0$

Contradiction, we have proved $n=0$, but have previously assumed $n \neq 0$.
$\therefore (m=0) \vee (n=0)$ holds true.