HOMEWORK 3

LEANDRO RIBEIRO
(WORKED WITH KYLE FRANKE AND JOYCE GOMEZ)

Axiom 1.2. *There exists an integer 0 such that whenever $m \in \mathbb{Z}$, m + 0 = m.*

Negation. For all integers n there exists some $m \in \mathbb{Z}$ such that m + n $\neq$ m

Axiom 1.3. *There exists an integer 1 such that 1 $\neq$ 0 and whenever $m \in \mathbb{Z}$, $m \cdot 1 = m$.*

Negation. For all integers n, n = 0 and there exists some $m \in \mathbb{Z}$ such that m $\cdot$ n $\neq$ m

Axiom 1.4. *For each $m \in \mathbb{Z}$, there exists an integer, denoted by -m, such that m + (-m) = 0.*

Negation. There exists some $m \in \mathbb{Z}$ such that for all integers denoted by -m, m + (-m) $\neq$ 0.

Axiom 1.5. *Let m, n, and p be integers. If $m \cdot n = m \cdot p$ and $m \neq 0$, then n = p.*

Negation. There exists some m, n, and p $\in \mathbb{Z}$ such that m $\cdot$ n = m $\cdot$ p and m $\neq$ 0, and n $\neq$ p.

Proposition 2.2. *For $m \in \mathbb{Z}$, one and only one of the following is true:*
(i) $m \in \mathbb{N}$
(ii) $-m \in \mathbb{N}$
(iii) m = 0.

Proof. Suppose first m = 0. By proposition 1.22, -0 = 0. Since 0 $\notin \mathbb{N}$, we can conclude that -0 $\notin \mathbb{N}$. Therefore both (ii) and (iii) fail. We may now assume that m $\neq$ 0. We argue by contradiction that m and -m are not both elements of $\mathbb{N}$. Suppose toward a contradiction that m $\in \mathbb{N}$ and -m $\in \mathbb{N}$. By our axiom for $\mathbb{N}$, $\mathbb{N}$ is closed under addition. m + (-m) $\in \mathbb{N}$. We infer that 0 $\in \mathbb{N}$. By our axiom, 0 $\notin \mathbb{N}$, so we have a contradiction. We conclude that m and -m are not both in $\mathbb{N}$. $\square$

Date: February 6, 2017.

Proposition 2.3. *$1 \in \mathbb{N}$*

Proof. Suppose toward a contradiction $1 \notin \mathbb{N}$. By our axiom, either $1 \in \mathbb{N}$, $1 = 0$, or $-1 \in \mathbb{N}$. We know $1 \neq 0$ by our axioms for the integers. We conclude that either $1 \in \mathbb{N}$ or $-1 \in \mathbb{N}$. Our reductio assumption implies $-1 \in \mathbb{N}$. The set $\mathbb{N}$ is closed under multiplication. Thus (-1)n is a natural number for any $n \in \mathbb{N}$. Then $(-1)(-1) \in \mathbb{N}$. By proposition 1.20, $(-1)(-1) = 1 \cdot 1 = 1$ by multiplicative identity. Therefore $1 \in \mathbb{N}$ by contradiction. $\square$

Proposition 2.7. *Let m, n, p, $q \in \mathbb{Z}$:*
(i) If $m < n$ then $m + p < n + p$.
(ii) If $m < n$ and $p < q$ then $m + p < n + q$.
(iii) If $0 < m < n$ and $0 < p \leq q$ then $mp < nq$.
(iv) If $m < n$ and $p < 0$ then $np < mp$.

Proof. (i) We observe $n - m \in \mathbb{N}$ by definition. Consider $n + p - (m + p) = n + p + -(m + p)$. By proposition 1.25.1, this is equal to $n + p - m - p$. We can rearrange this using commutativity to be $n - m + p - p$. After applying axiom 1.4, we know $n - m + p - p = n - m + 0 = n - m$ by axiom 1.2. Since $n - m \in \mathbb{N}$, we conclude that $n + p - (m + p) \in \mathbb{N}$, so $m + p < n + p$.

(ii) Observe that $n - m \in \mathbb{N}$ and $q - p \in \mathbb{N}$. Consider $n + q - (m + p) = n + q + -(m + p)$. By axiom 1.25.1, $n + q + -(m + p) = n + q - m - p$. After applying commutativity and associativity, we can see that $n + q - m - p = (n - m) + (q - p)$. Since $\mathbb{N}$ is closed under addition and $(n - m) \in \mathbb{N}$ and $(q - p) \in \mathbb{N}$, we conclude $(n - m) + (q - p) \in \mathbb{N}$. Therefore $m + p < n + q$.

(iii) We're given $0 < m$, $m < n$, $0 < p$, and $p \leq q$. Let's make several observations. Since $0 < m$, $m - 0 \in \mathbb{N}$. As $m - 0 = m$ by the identity element of addition, we conclude $m \in \mathbb{N}$. Since $m < n$, we also have that $m - n \in \mathbb{N}$. Since $0 < p$, we have $p - 0 \in \mathbb{N}$, so $p \in \mathbb{N}$. We finally have that $p \leq q$. Hence either $p < q$ or $p = q$. We here have two cases.

Case 1: $p = q$ holds. Consider $nq - mp$. Observe that $nq - mp = nq - mq$. Factoring, we have that $nq - mq = (n - m)q$. By our observations, $p \in \mathbb{N}$. Since $\mathbb{N}$ is closed under multiplication, $(n - m)q \in \mathbb{N}$. We deduce that $nq - mp \in \mathbb{N}$. Hence $mp < nq$.

Case 2: $p < q$ holds. We have $q - p \in \mathbb{N}$. Consider $nq - mp$. Clearly $nq - mp = nq - mq + mq - mp$. $nq - mq + mq - mp = (n - m)q + m(q - p)$. We have that $m \in \mathbb{N}$, $n - m \in \mathbb{N}$, and $q - p \in \mathbb{N}$. We also see that $0 < p < q$, so $0 < q$ by transitivity of $<$, therefore $q = q - 0 \in \mathbb{N}$. Since $\mathbb{N}$ is closed under multiplication and addition we infer that $(n - m)q + m(q - p) \in \mathbb{N}$. Therefore, $nq - mp \in \mathbb{N}$, so $mp < nq$.

(iv) Let's make several observations. n - m $\in \mathbb{N}$, and 0 - p $\in \mathbb{N}$ by definition. Thus -p $\in \mathbb{N}$. -p(n - m) $\in \mathbb{N}$, because $\mathbb{N}$ is closed under multiplication. By distributivity, -pn + (-p)(-m) $\in \mathbb{N}$. By proposition 1.25, -pn +(-p)(-m) = (-1)pn + (-1)p(-1)m $\in \mathbb{N}$. By cor 1.21 (-1)(-1) = 1. We have that 1 $\cdot$ mp + -(np) $\in \mathbb{N}$ by 1.25, we conclude that mp - np $\in \mathbb{N}$. Therefore mp < np. ☐

Proposition 2.8. *Let m,n $\in \mathbb{Z}$. Exactly one of the following is true: m < n, m = n, m > n.*

Proof. Let's first observe the first case, m < n. By definition, this means that n - m $\in \mathbb{N}$. Proposition 2.2 states that -(n - m) $\notin \mathbb{N}$ and n - m $\neq$ 0. -(n - m) = -(n + (-m)) = (-1)(n + (-m)) by proposition 1.25. We can then distribute and see that (-1)(n + (-m)) = (-1)n + (-1)(-m). After reapplying 1.25, (-1)n + (-1)(-m) = -n + m. -n + m = m - n by commutativity and the definition of subtraction. Therefore -(n - m) = (m - n) $\notin \mathbb{N}$. This means m $\not>$ n. n - m $\neq$ 0 tells us that m $\neq$ n, as they are not additive inverses.

In the event that m = n, we know that m - n = m - m = m + (-m) = 0 thanks to the additive inverse axiom. 2.2 also tells us that m - n $\notin \mathbb{N}$ and its negation, n - m $\notin \mathbb{N}$. Therefore m $\not>$ n and m $\not<$ n.

Finally, in the event that m > n we know that m - n $\in \mathbb{N}$. Proposition 2.2 states that -(m - n) $\notin \mathbb{N}$ and m - n $\neq$ 0. -(m - n) = -(m + (-n)) = (-1)(m + (-n)) by proposition 1.25. We can then distribute and see that (-1)(m + (-n)) = (-1)m + (-1)(-n). After reapplying 1.25, (-1)m + (-1)(-n) = -m + n. -m + n = n - m by commutativity and the definition of subtraction. Therefore -(m - n) = (n - m) $\notin \mathbb{N}$. This means m $\not<$ n. m - n $\neq$ 0 tells us that m $\neq$ n, as they are not additive inverses. ☐

Proposition 2.10. *The equation x^2 = -1 has no solution in $\mathbb{Z}$.*

Proof. Suppose towards a contradiction that x^2 = -1 has a solution in $\mathbb{Z}$. By definition, this means x $\cdot$ x = -1. Let m $\in \mathbb{Z}$ and m $\neq$ 0. Suppose m $\in \mathbb{N}$. Because $\mathbb{N}$ is closed under multiplication m^2 = m $\cdot$ m $\in \mathbb{N}$. On the other hand, suppose -m $\in \mathbb{N}$. By proposition 1.20, m^2 = m $\cdot$ m = (-m)(-m) $\in \mathbb{N}$, thanks to $\mathbb{N}$ being closed under multiplication. We conclude $m^2 \in \mathbb{N}$ for all m $\in \mathbb{Z}$ if m $\neq$ 0. Therefore, x $\in \mathbb{Z}$ which means -1 $\in \mathbb{N}$, which is absurd since -1 < 0, so it is a negative integer. By definition $\mathbb{N}$ only contains positive integers. ☐

Proposition 2.12. *For all m, n, p $\in \mathbb{Z}$:*
(i) -m < -n if and only if m > n.
(ii) If p > 0 and mp < np then m < n.

(iii) If $p < 0$ and $mp < np$ then $n < m$.
(iv) If $m \leq n$ and $0 \leq p$ then $mp \leq np$.

Proof. (i) Let's first prove that if -m < -n, then m > n. By definition, -n - (-m) $\in \mathbb{N}$. That is, -n + -(-m) $\in \mathbb{N}$. Appealing to prop. 1.22, -(-m) = m. We conclude that -n + m $\in \mathbb{N}$. By commutativity, m - n $\in \mathbb{N}$, hence n < m. We need to prove the other implication. That is, if n < m, then -m < -n. By definition, m - n $\in \mathbb{N}$. By commutativity, m - n = -n + m. Using proposition 1.22 m = -(-m), so -n + -(-m) $\in \mathbb{N}$. By definition, -n - (-m) $\in \mathbb{N}$. Therefore, -m < -n.

(ii) We have p > 0, so p - 0 $\in \mathbb{N}$ and therefore p $\in \mathbb{N}$. By definition, np - mp $\in \mathbb{N}$. np - mp = np + -mp. By proposition 1.2, np + -mp = (n + -m) $\cdot$ p. Appealing to commutativity, p(n - m) $\in \mathbb{N}$. By proposition 2.11(proved below), we conclude that n - m $\in \mathbb{N}$. Therefore m < n.

(iii)We have p < 0, so 0 - p = 0 + (-p) $\in \mathbb{N}$ and therefore (-p) $\in \mathbb{N}$ by proposition 1.7. By definition, n(-p) - m(-p) $\in \mathbb{N}$. n(-p) - m(-p) = n(-p) + -m(-p) = n(-p) + mp by proposition 1.20. By proposition 1.2 and 1.25, n(-p) + mp = -np + mp = (-n + m) $\cdot$ p. Appealing to commutativity, p(m + -n) $\in \mathbb{N}$. By proposition 2.11(proved below), we conclude that m - n $\in \mathbb{N}$. Therefore n < m.

(iv)Here we have several different cases to consider.

Case 1. p = 0. m $\cdot$ 0 = n $\cdot$ 0 = 0 by proposition 1.14, therefore mp = np.

Case 2. m = n. By applying the additive inverse, we can see that n - m = 0. We can multiply p on both sides on the left to get p(n - m) = p $\cdot$ 0 = 0. If we distribute we can see mp - np = 0. This means mp = np by definition.

Case 3. m < n. By definition, this means n - m $\in \mathbb{N}$. Because p - 0 = p $\in \mathbb{N}$ by our axioms for the integers, p(n - m) $\in \mathbb{N}$ because $\mathbb{N}$ is closed under multiplication. If we distribute and apply commutativity, p(n - m) = p(n + -m) = pn - pm = np - mp $\in \mathbb{N}$. This means mp < np by definition. ☐

Proposition 2.11. *Let $m \in \mathbb{N}$ and $n \in \mathbb{Z}$. If $m \cdot n \in \mathbb{N}$, then $n \in \mathbb{N}$.*

Proof. By proposition 2.2, exactly one of the following hold: n = 0, n $\in \mathbb{N}$, or -n$\in \mathbb{N}$.

Case 1. n = 0. Since n = 0, m $\cdot$ 0 $\in \mathbb{N}$. By proposition 1.14, m $\cdot$ 0 = 0. Therefore, 0 $\in \mathbb{N}$, which is absurd. We conclude that this is impossible.

Case 2. n $\in \mathbb{N}$. Since we're trying to prove this, we're done.

Case 3 -n $\in \mathbb{N}$. Since m $\in \mathbb{N}$, m $\cdot$ (-n) $\in \mathbb{N}$ because $\mathbb{N}$ is closed under multiplication. m $\cdot$ n + m(-n) $\in \mathbb{N}$ because $\mathbb{N}$ is closed under addition.

Using distributivity, $m(n + (-n)) \in \mathbb{N}$. Thus $m \cdot 0 \in \mathbb{N}$, but this implies $0 \in \mathbb{N}$, which is absurd. $\square$