Assignment 02

Naman Mishra

31 October 2022

Problem 1.

(a) Prove that for any $m, n \in \mathbb{N}$, exactly one of the following statements holds.

  (*i*) $m = n$;

  (*ii*) there is a $k \in \mathbb{N} \setminus \{0\}$ such that $m + k = n$;

  (*iii*) there is a $k \in \mathbb{N} \setminus \{0\}$ such that $n + k = m$.

  You may use: induction, the definition of sum_m any of its six properties stated in class (as Theorem 1.12), and the fact that the range of the function $f(x) = x+1$ on $\mathbb{N}$ is $\mathbb{N} \setminus \{0\}$ (Problem 1 in HW1).

(b) Show that $\mathbb{N}$ is an ordered set if we define $<$ as follows: $m < n$ if there is a $k \in \mathbb{N} \setminus \{0\}$ such that $m + k = n$.

Proof. Unless otherwise stated, any lowercase variable denotes a natural number.

(a) Let $R \subseteq \mathbb{N} \times \mathbb{N}$ be a relation such that $a\ R\ b \Leftrightarrow \exists\ k \neq 0$ such that $a + k = b$. Let

$$B = \{m \in \mathbb{N} : m = n, m\ R\ n, \text{ or } n\ R\ m\}$$

Note: If $\exists\ k$ such that $m + k = n$, then $m \in B$ as $k = 0$ gives $m = n$ and $k \neq 0$ gives $m\ R\ n$. Similarly $n + k = m$ also implies $m \in B$.
$0 \in B$ as $0 + n = n$.
If $b \in B$, then:

($b = n$) $S(b) = S(n) = n + 1 \Rightarrow S(b) \in B$.

($b\ R\ n$) $\exists\ k \neq 0$ such that $b + k = n$. Since $k \in \text{ran}(S)$ (HW 1.1), $\exists\ k'$ such that $S(k') = k$. Thus $b + S(k') = n \Rightarrow S(b) + k' = n \Rightarrow S(b) \in B$.

($n\ R\ b$) $\exists\ k \neq 0$ such that $n + k = b$. Then $S(n + k) = S(b) \Rightarrow n + S(k) = S(b) \Rightarrow S(b) \in B$.

Thus $b \in B \Rightarrow S(b) \in B \Rightarrow B = \mathbb{N}$. Since n was arbitrary, one of the three statements holds for each m, n.
Suppose $m = n$. Then if $m + k = n$, then $m + k = m + 0 \Rightarrow k = 0$ by the cancellation law. Similarly $n + k = m$ also implies $k = 0$. Thus $m = n$ cannot

hold simultaneously with $m\ R\ n$ or $n\ R\ m$. Now if $m + k = n$ and $n + k' = m$, then $(n + k') + k = n \Rightarrow n + (k + k') = n + 0 \Rightarrow k + k' = 0 \Rightarrow k = k' = 0$. Thus $m\ R\ n$ and $n\ R\ n$ cannot hold simultaneously.
Therefore exactly one of the three statements holds for all $m, n \in \mathbb{N}$

(b) If we define $m < n$ as $m\ R\ n$ above, from part (a) it is clear that exactly one of $m = n, m < n, n < m$ holds for all $m, n \in \mathbb{N}$. Moreover, if $a < b$ and $b < c$, then there exist natural numbers $k, k' \neq 0$ such that $a + k = b$ and $b + k' = c$. This implies $(a + k) + k' = a + (k + k') = c$. Since $x + y = 0 \Rightarrow x = y = 0$, $x \neq 0$ or $y \neq 0 \Rightarrow x + y \neq 0$. Thus $k + k' \neq 0 \Rightarrow a < c$.
We have shown that $<$ obeys trichotomy and is transitive. Thus $(\mathbb{N}, <)$ is an ordered set. □

Problem 2. Let $(F, +, \cdot)$ be a field. According to axiom (F5), given $x \in F$, there is a $y \in F$ such that $x + y = 0$. Show that y is unique, i.e., if there is a $z \in F$ such that if $x + y = x + z = 0$, then $y = z$. Use only the field axioms to justify your answer.

Proof.

$$\begin{aligned} x + y &= x + z \\ (y + x) + y &= (y + x) + z \\ y &= z \end{aligned}$$

□

Problem 3. Let $+$ and $\cdot$ be the usual addition and multiplication on $\mathbb{N}$. You are free to use their well-known properties.

(a) Let $F = \{0, 1, 2, 3\}$. We endow F with addition and multiplication as follows:

$a \oplus b = c$, where c is the remainder that $a + b$ leaves when divided by 4

$a \odot b = c$, where c is the remainder that $a \cdot b$ leaves when divided by 4

Is $(F, \oplus, \odot)$ a field? Please justify your answer.

(b) Let $F = \{0, 1\}$. We endow F with addition and multiplication as follows:

$a \oplus b = c$, where c is the remainder that $a + b$ leaves when divided by 2

$a \odot b = c$, where c is the remainder that $a \cdot b$ leaves when divided by 2

You may assume that $(F, \oplus, \odot)$ is a field. Is it possible to give F a relation $<$ so that $(F, \oplus, \odot, <)$ is an ordered field? Please justify your answer.

Proof. (a) Clearly 1 is the multiplicative identity.

$$\begin{array}{cccc} 2 \cdot 0 = 0 & 2 \cdot 1 = 2 & 2 \cdot 2 = 4 & 2 \cdot 3 = 6 \\ 2 \odot 0 = 0 & 2 \odot 1 = 2 & 2 \odot 2 = 0 & 2 \odot 3 = 2 \end{array}$$

Thus there is no multiplicative inverse of 2 in F. So $(F, \oplus, \odot)$ is not a field.

(b) If $(F, \oplus, \odot, <)$ is an ordered field and $0 < 1$, then by the field axioms, $0 \oplus 1 < 1 \oplus 1 \Leftrightarrow 1 < 0$ which is a contradiction as it disobeys trichotomy of order. If $1 < 0$ then $1 \oplus 1 < 0 \oplus 1 \Leftrightarrow 0 < 1$, which cannot be true. □

Problem 4. Let $(F, +, \cdot, <)$ be an ordered field.

(i) Using only the field axioms, and the uniqueness of the additive inverse, show that for all $a, b, c \in F, a(b - c) = ab - ac$.

(ii) Using the field axioms, the order axioms, and Part (i), show that for all $a, b, c \in F$, if $a < b$ and $c < 0$, then $bc < ac$.

Proof. (i) $a(b + (-c)) = ab + a(-c)$

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

Thus $a(b + (-c)) = ab - ac$.

(ii) $c < 0 \Rightarrow c + (-c) < -c \Rightarrow 0 < -c$.
$a < b \Rightarrow a + (-a) < b + (-a) \Rightarrow 0 < b - a$.
Thus

$$\begin{aligned} &0 < (b + (-a))(-c) && \text{(O4)} \\ &0 < b(-c) + (-a)(-c) \\ &0 < -bc + ac \\ &bc < ac \end{aligned}$$

□

Problem 5. Apostol defines an ordered field as a field $(F, +, \cdot)$ together with a set $P \subseteq F$ satisfying the following axioms.

(O'1) If $x, y \in P$, then $x + y \in P$ and $x \cdot y \in P$.

(O'2) For every $x \in F$ such that $x \neq 0$, $x \in P$ or $-x \in P$, but not both.

(O'3) $0 \notin P$

Show that our definition of an ordered field is equivalent to that of Apostol's. That is, show that for a field$(F, +, \cdot)$:

(i) If there is a relation $<$ satisfying (O1)-(O4), then there is a $P \subseteq F$ satisfying (O'1)-(O'3), and

(ii) if there is a $P \subseteq F$ satisfying (O'1)-(O'3), then there is a relation $<$ satisfying (O1)-(O4).

Proof. Suppose there is a relation $<$ on $(F, +, \cdot)$ satisfying (O1)-(O4). Define

$$P = \{x \in F : 0 < x\}$$

Suppose $x, y \in P \Leftrightarrow 0 < x, y$. Then $-x < x + (-x) \Rightarrow -x < 0 < y \Rightarrow -x < y \Rightarrow 0 < x + y \Rightarrow x + y \in P$ by (O2) and (O3).
If $x, y \in P$, then by (O4), $x \cdot y \in P$.
Thus (O'1) holds.

If $0 < x$, $x \in P$. If $x < 0$, then by (O3) $x + (-x) < -x \Rightarrow 0 < -x$, *i.e.*, $-x \in P$. Thus (O'2) is holds.

$0 \not< 0$, so (O'3) holds.

Now suppose there is a subset $P \subseteq F$ which satisfies (O'1)-(O'3). Define relation $<$ on F as $a < b \Leftrightarrow b - a \in P$.
Note that $-(b - a) = a - b$.

(O1) For any $a, b \in F$, exactly one of $b - a = 0$, $b - a \in P$, and $-(b - a) \in P$ holds (by (O'2) and (O'3), as $-0 = 0$). $b - a = 0 \Leftrightarrow a = b, b - a \in P \Leftrightarrow a < b$, and $-(b - a) \in P \Leftrightarrow a - b \in P \Leftrightarrow b < a$. Thus exactly one of $a = b, a < b$, and $b < a$ holds.

(O2) If $a < b$ and $b < c$, then $b - a \in P$ and $c - b \in P$. So by (O'1), $c - b + b - a \in P \Leftrightarrow c - a \in P \Leftrightarrow a < c$.

(O3) If $a < b$ and $c \in F$, then $(b + c) - (a + c) = b + c + (-a) + (-c) = b - a \in P \Rightarrow a + c < b + c$.

(O4) $0 < a \Leftrightarrow a - 0 \in P \Leftrightarrow a \in P$. So $0 < a$ and $0 < b$ implies $0 < a \cdot b$ by (O'1). $\square$