UM 101 HOMEWORK ASSIGNMENT 2

SKETCH OF SOLUTIONS

Problem 1. (a) Prove that for any $m, n \in \mathbb{N}$, exactly one of the following statements hold.

(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 and 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).

Sketch of Solution. Step 1. At most one of the statements hold.

- Suppose $m = n$ and $m + k = n$ for some $k \in \mathbb{N} \setminus \{0\}$. Then, $m + k = n + 0$ and by cancellation, $k = 0$. This is a contradiction.
- The same argument shows that (i) and (iii) cannot occur simultaneously.
- Suppose $m + k_1 = n$ for some $k_1 \in \{0\}$ and $n + k_2 = m$ for some $k_2 \in \{0\}$. Then, $m + k_1 + k_2 = m + 0$. By cancellation, $k_1 + k_2 = 0$, which implies that $k_1 = k_2 = 0$. Contradiction.

Step 2. At least one of the statements holds. Fix $n \in \mathbb{N}$. We prove the statement $P_m(n)$ by inducting on m, where

$$P_n(m): \text{ at least one of } (i), (ii) \text{ or } (iii) \text{ hold.}$$

Claim (Base case). $P_n(0)$ is true.

Proof. **Case I.** If $n = 0$, then $n = m = 0$, hence (i) holds.
Case II. If $n \neq 0$, set $k = n$. Then $n = n + 0 = k + m$. Hence, (ii) holds. □

Claim (Inductive case). If $P_n(m)$ holds, then $P_n(m + 1)$ holds.

Proof. IDEA: For each of $m = n$, $m + k = n$ for some $k \in \mathbb{N} \setminus \{0\}$ and $n + k = m$ for some $k \in \mathbb{N} \setminus \{0\}$, show what relationship it implies between n and $m + 1$. □

(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 $m + k = n$.

Sketch of Solution. We need to establish (O1) and (O2). (O1) was already established in Part (a) For [(O2)], let $m, n, l \in N$ such that $m+k_1 = n$ and $n+k_2 = l$ for some $k_1, k_2 \in \mathbb{N}\backslash\{0\}$. Then, $m + k_1 + k_2 = l$.

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 $x+y = x+z = 0$, then $y = z$. Use only the field axioms to justify your answer.

Given. For every $x \in F$, there exists a $y \in F$ such that $x + y = 0$.
To show. Given x such a y is unique, i.e if $z \in F$ such that $x + z = 0$, then $y = z$.
Proof. By (F4), $y = y + 0.$,
Since $x + z = 0$, $y = y + (x + z)$,
By (F2), $y = (y + x) + z$,
By (F1), $y = (x + y) + z$,
Since $x + y = 0$, $y = z$.

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.

$$a \oplus b = c, \quad \text{where } c \text{ is the remainder that } a + b \text{ leaves when divided by 4,}$$
$$a \odot b = d, \quad \text{where } d \text{ is the remainder that } a \cdot b \text{ leaves when divided by 4.}$$

Is $(F, \oplus, \odot)$ a field? Please justify your answer.
Sketch of Solution. First show (by direct computation) that 1 is a multiplicative inverse. Next, show that 2 has no multiplicative inverse by multiplying with each element of the set F.
(b) Let $F = \{0, 1\}$. We endow F with addition and multiplication as follows.

$$a \oplus b = c, \quad \text{where } c \text{ is the remainder that } a + b \text{ leaves when divided by 2,}$$
$$a \odot b = d, \quad \text{where } d \text{ is the remainder that } a \cdot b \text{ leaves when divided by 2.}$$

You may assume $(F, \oplus, \odot)$ is a field (or treat this as an additional exercise, but this won't appear on your quiz). Is it possible to give F a relation $<$ so that $(F, \oplus, \odot, <)$ is an ordered field? Please justify your answer.

Sketch of Solution. Suppose F admits relation $<$ so that $(F, \oplus, \odot, <)$ is an ordered field. We know that in an ordered Field $0 < 1$. Now by (O3) we have that $0 \oplus 1 < 1 \oplus 1$. But $1 \oplus 1 = 0$, hence we get $1 < 0$, a contradiction to the Law of Trichotomy, i.e., (O1).

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) By distributivity, $a(b-c) = a \cdot b + a \cdot (-c)$. Thus, we must show that $a \cdot (-c) = -a \cdot c$. For this, observe that $ac + a(-c) = a(c - c) = a \cdot 0 = 0$. Thus, by the uniquess of additive inverse, $a \cdot (-c) = -(a \cdot c)$

(ii) Adding (the unique) additive inverses, we get that $0 < b - a$ and $0 < -c$. By (O3), $0 < -c \cdot (b - a) = (-c) \cdot b + (-c) \cdot (-a)$. We proved in the last part that $(-c)\dot{b} = -bc$ and $(-c) \cdot (-a) = -(c \cdot (-a)) = ca$. Thus, $0 < c(a - b) = ca - cb$. Now, we add bc on both sides. □

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 $x \neq 0$, either $x \in P$ 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. (i) We are given that there is a relation $<$ satisfying O1- O4. We need to prove that there is a $P \subseteq F$ satisfying (O'1)- (O'3). No define a subset P of F as

$$P = \{x \in F : x > 0\}.$$

We will establish the four axioms (O'1)- (O'3) for this set.

(1) By O4 we have that if $x, y \in P$ then $x.y \in P$. We need to show now that $x + y \in P$. Let $c = x + y$. We will have two cases. First when $c = 0$, implies $x + y = 0$. By Cancellation Law for Addition we have $x = -y$. Now as $y > 0$, implies $-y < 0$, which further implies that $x < 0$, a contradiction to the fact that $x \in P$. Hence we cannot take $c = 0$. Second case we take $c \neq 0$. By O1 either $c > 0$ or $c < 0$. Now if $c > 0$, then we are done. If $c < 0$, that means $x + y < 0$. By O3, adding $-y$ on both sides we get $x < -y$. This again implies that $x < 0$, a contradiction to the fact that $x \in P$.

(2) If $x \in F$, then by O1, either $x = 0$ or $x > 0$ or $x < 0$. We are given that $x \neq 0$, so we have two cases remaining. If $x > 0$, then $x \in P$. If $x < 0$, then $-x > 0$ (prove it), which means that $-x \in P$.

(3) By O1 we have that if $x = 0$, then $x > 0$ is not possible. Therefore $0 \notin P$.

(ii) Given $x, y \in F$, we say that

$$x < y \quad \text{if} \quad y - x \in P.$$

We will establish the four axioms O1-O4 for this relation.

(1) Let $x, y \in F$. First, suppose $x = y$. Then, since $0 \notin P$, neither $y - x \in P$ nor $x - y \in P$. Next, suppose $x \neq y$. Let $z = y - x$. By (O'2), either $z \in P$ or $-z \in P$ but not both. If $z \in P$, then $x < y$. If $-z = x - y \in P$, then $y < x$.

(2) Let $x, y, z \in F$ such that $x < y$ and $y < z$. Then, $y - x \in P$ and $z - y \in P$. Thus, by (O'1), $(z - y) + (y - x) = z - x \in P$. Thus, $x < z$.

(3) Let $x, y, z \in F$ such that $x < y$. Then, $y - x \in P$. Now, $(y + z) - (x + z) = y - x \in P$. Thus, $x + z < y + z$.

(4) Let $x, y \in F$ such that $0 < x$ and $0 < y$. Then, $x, y \in P$. Thus, by (O'1), $xy \in P$. Thus, $xy > 0$.

$\square$