MATH 0450: HOMEWORK 3

TEOH ZHIXIANG

Problem 1. Let $L = \{q \in \mathbb{Q} \mid q^2 < 2\}$. Show that if $q > 0$ and $q \in L$ then $q' = 2(q+1)/(q+2) \in L$ and $q < q'$. Deduce that L does not have a maximal element.

Proof.

$$\begin{aligned}
(q')^2 &= \frac{(2(q+1))^2}{(q+2)^2} \\
&= \frac{4q^2+8q+4}{q^2+4q+4} \\
&= \frac{q^2+4q+4+3q^2+4q}{q^2+4q+4} \\
&= 1 + \frac{3q^2+4q}{q^2+4q+4} \\
&= 1 + \frac{(q^2+4q)+2q^2}{(q^2+4q)+4} \\
&< 1+1 \\
&= 2
\end{aligned}$$

$q' = \frac{2(q+1)}{q+2} \in \mathbb{Q}$ if $q \in \mathbb{Q}$, and $(q')^2 < 2$ if $q \in L$ as shown above, so $q' \in L$.

$$\begin{aligned}
q' &= \frac{2q+2}{q+2} \\
&= \frac{q(q+2)+2-q^2}{q+2} \\
&= q + \frac{2-q^2}{q+2} \\
&> q
\end{aligned}$$

since $q^2 < 2 \Leftrightarrow 2 - q^2 > 0$ and $q > 0 \Leftrightarrow q + 2 > 0$. So $q < q'$.

Given any $q \in L$ we can recursively, using the formula for q' above, derive a $q' > q \in L$, and likewise for $q'' > q'$, $q''' > q''$, and so on. Since for every $q \in L$ we can keep constructing a $q < q' \in L$, this shows there is always a greater element $q' > q \in L$ for every q, and that there is no maximal element in L. $\square$

Problem 2. Let $U = \{u \in \mathbb{Q} \mid u^2 \geq 2\}$. Show that if $u > 0$ and $u \in U$ then $u' = 2(u+1)/(u+2) \in U$ and $u > u'$. Deduce that U does not have a minimal element.

Date: February 6, 2020.

Proof.

$$\begin{aligned}
(u')^2 &= \frac{(2(u+1))^2}{(u+2)^2} \\
&= \frac{4u^2+8u+4}{u^2+4u+4} \\
&= \frac{u^2+4u+4+3u^2+4u}{u^2+4u+4} \\
&= 1+\frac{3u^2+4u}{u^2+4u+4} \\
&= 1+\frac{(u^2+4u)+2u^2}{(u^2+4u)+4} \\
&\geq 1+1 \\
&= 2
\end{aligned}$$

$u' = \frac{2(u+1)}{u+2} \in \mathbb{Q}$ if $u \in \mathbb{Q}$, and $(u')^2 \geq 2$ if $u \in U$ as shown above, so $u' \in L$.

$$\begin{aligned}
u' &= \frac{2u+2}{u+2} \\
&= \frac{u(u+2)+2-u^2}{u+2} \\
&= u+\frac{2-u^2}{u+2} \\
&< u
\end{aligned}$$

since $u^2 > 2 \Leftrightarrow 2-u^2 < 0$ and $u > 0 \Leftrightarrow u+2 > 0$. So $\frac{2-u^2}{u+2} < 0$, and $u > u'$.

Given any $u \in U$ we can recursively, using the formula for u' above, derive a $u' < u \in U$, and likewise for $u'' < u'$, $u''' < u''$, and so on. Since for every $u \in U$ we can keep constructing a $u' < u \in U$, this shows there is always a smaller rational element $u' < u \in U$ for every u, and that there is no minimal element in U. □

Problem 3. Let F be an ordered field. Show that for any $n \geq 1$ and $a_1, a_2, \ldots, a_n \in F$ we have

$$|a_1+a_2+\cdots+a_n| \leq |a_1|+|a_2|+\cdots+|a_n|.$$

Proof. (By induction). We first define the absolute value operation $|\cdot|$ as follows:

$$|a| = \begin{cases} a & \text{if } a > 0 \\ -a & \text{if } a < 0 \\ 0 & \text{if } a = 0 \end{cases}$$

Let $P(n)$ be the statement $|a_1+a_2+\cdots+a_n| \leq |a_1|+|a_2|+\cdots+|a_n|$, for $n \geq 1$ and $a_1, a_2, \ldots, a_n \in F$. We prove two base cases: $P(1)$ and $P(2)$. The first base case, $P(1)$, is trivial because $|a_1| = |a_1| \Leftrightarrow |a_1| \leq |a_1|$. We shall prove $P(2)$, also called the triangle inequality, i.e. $|a_1+a_2| \leq |a_1|+|a_2|$. By definition of absolute value operation, $|a_1 + a_2| \geq 0$, and $|a + b| \geq 0$. Note also

$$
\begin{aligned}
|a|^2 &= |a| \cdot |a| \\
\text{consider 3 cases:} & \\
a > 0 : |a|^2 &= a \cdot a \\
&= a^2 \\
a < 0 : |a|^2 &= -a \cdot -a \\
&= a^2 \text{ (by property of ordered field } -a \cdot -b = a \cdot b) \\
a = 0 : |a|^2 &= 0 \cdot 0 \\
&= a^2 \\
\Rightarrow |a|^2 &= a^2
\end{aligned}
$$

Therefore

$$
\begin{aligned}
& & |a_1 + a_2| &\leq |a_1| + |a_2| \\
&\Leftrightarrow & (a_1 + a_2)^2 &\leq (|a_1| + |a_2|)^2 \\
&\Leftrightarrow & a_1^2 + a_2^2 + 2a_1a_2 &\leq |a_1|^2 + |a_2|^2 + 2|a_1||a_2| \\
& & &= a_1^2 + a_2^2 + 2|a_1||a_2| \\
&\Leftrightarrow & 2a_1a_2 &\leq 2|a_1||a_2| \\
&\Leftrightarrow & a_1a_2 &\leq |a_1||a_2|
\end{aligned}
$$

Note $|a_1||a_2| = |a_1a_2|$: consider cases for different values of a_1, a_2. If $a_1, a_2 > 0$ or $a_1, a_2 < 0$, statement valid. (a_1 or $a_2 = 0$) $\Rightarrow |0| = |0|$ valid. If only either a_1 or $a_2 < 0$: assume $a_2 < 0$, $|a_1||a_2| = a_1(-a_2) = |-a_1a_2| > 0$, similarly for $a_1 < 0$. Therefore $a_1a_2 \leq |a_1||a_2|$ true, and $P(2)$ valid.

Next we assume $P(n)$ true for some $n \in \mathbb{N}$. Then

$$
\begin{aligned}
& & |\underbrace{a_1 + a_2 + \cdots + a_n}_{:=\text{ A}} + a_{n+1}| &\leq |\underbrace{a_1 + a_2 + \cdots + a_n}_{:=\text{ A}}| + |a_{n+1}| \\
&\Leftrightarrow & |A + a_{n+1}| &\leq |A| + |a_{n+1}|
\end{aligned}
$$

By $P(2)$, the above inequality in A is true. In a similar manner to the above, $P(n+1)$ can be proven in a recursive manner:

$$
\begin{aligned}
|A| + |a_{n+1}| &= |a_1 + a_2 + \cdots + a_{n-1} + a_n| + |a_{n+1}| \\
&\leq |\underbrace{a_1 + a_2 + \cdots + a_{n-1}}_{A_2} + a_n| + |a_{n+1}| \\
&\leq |A_2| + |a_n| + |a_{n+1}| \\
&\leq \ldots
\end{aligned}
$$

each time using result from $P(2)$. Therefore $P(n+1)$ true, and so by Principle of Mathematical Induction $P(n)$ true for all $n \in \mathbb{N}$. $\square$

Problem 4. Let A and B be two sets with n and, respectively, m elements. Let $f : A \to B$ a function. Show that

(1) If f injective then $n \leq m$;
(2) If f surjective then $n \geq m$;
(3) If f bijective then $n = m$.

Proof. (1) (Contraposition). f is said to be injective or 1-1 if for every two elements $a, b \in A$, $(f(a) = f(b)) \Rightarrow (a = b)$. Assume negation of $n \leq m$ is true, i.e. $n > m$. If f is injective, then every two elements $a_1, a_2 \in A$ must have different images $b_1, b_2 \in B$ under f, if $f(a_1) = b_1$ and $f(a_2) = b_2$. Pigeonhole principle states that if $n > m$ containers are put into m containers then at least one container must contain more than one item. So because the cardinality of the domain $|A| = n$ is greater than the cardinality of the codomain $|B| = m$, as assumed, by pigeonhole principle, there is no way to map $n > m$ elements in domain A to m elements in domain B without at least one element in domain B having more than one preimage from domain A. So f is shown to not be injective, and by proof of contraposition we have that f injective $\Rightarrow n \leq m$.

(2) (Contraposition). f is said to be surjective or onto if every element $b \in B$ has a preimage $a \in A$. Assume $n < m$. The function f is defined as the relation between sets A and B that associates every element in domain A to exactly one element in the codomain B. Hence, similarly by pigeonhole principle, we see that there is no way to map $n < m$ elements in domain A to m elements in domain B without at least one element in domain A mapping to two elements in codomain B, which defies the definition of a function. Thus f cannot be surjective, and by proof of contraposition we have that f surjective $\Rightarrow n \geq m$.

(3) Let $p \Rightarrow (r \vee s)$ be the statement in part (1) and $q \Rightarrow (r \vee t)$ be the statement in part (2), where p, q, r, t, s represent the statements "f injective", "f surjective", "$n = m$", "$n < m$" and "$n > m$" respectively. Hence we can introduce a third proposition $\neg((n < m) \wedge (n > m)) \equiv \neg(s \wedge t) \equiv \neg s \vee \neg t$.

Now we set up a proof by cases with our three propositional statements, considering the two cases: when $\neg s$ and when $\neg t$. The following is a First Order Logic (FOL) proof in fitch format:

1	$p \Rightarrow (r \vee t)$	
2	$q \Rightarrow (r \vee s)$	
3	$\neg s \vee \neg t$	
4	$\quad \neg t$	
5	$\quad\quad p \wedge q$	
6	$\quad\quad p$	$\wedge$E, 5
7	$\quad\quad r \vee t$	$\Rightarrow$E, 1, 6
8	$\quad\quad\quad r$	
9	$\quad\quad\quad r$	R, 8
10	$\quad\quad\quad t$	
11	$\quad\quad\quad \neg t$	R, 10
12	$\quad\quad\quad \perp$	$\neg$E, 10, 11
13	$\quad\quad\quad r$	$\perp$E, 12
14	$\quad\quad r$	$\vee$E, 7, 8–9, 10–13
15	$\quad (p \wedge q) \Rightarrow r$	$\Rightarrow$I, 5–14
16	$\quad \neg s$	
17	$\quad\quad p \wedge q$	
18	$\quad\quad q$	$\wedge$E, 17
19	$\quad\quad r \vee s$	$\Rightarrow$E, 2, 18
20	$\quad\quad\quad r$	
21	$\quad\quad\quad r$	R, 20
22	$\quad\quad\quad s$	
23	$\quad\quad\quad \neg s$	R, 22
24	$\quad\quad\quad \perp$	$\neg$E, 22, 23
25	$\quad\quad\quad r$	$\perp$E, 24
26	$\quad\quad r$	$\vee$E, 16, 20–21, 22–25
27	$\quad (p \wedge q) \Rightarrow r$	$\Rightarrow$I, 17–26
28	$(p \wedge q) \Rightarrow r$	$\vee$E, 3, 4–15, 16–27

And from this we can see that statement (3): f bijective $\Rightarrow n = m$ follows from statements (2) and (3).

□

Problem 5. The set S is said to be infinite if there exists a proper subset $A \subseteq S$ and an injective function $S \to A$. Show that the sets $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are infinite.

Proof. The set A is defined to be a proper subset of S, $A \subset S$, if it satisfies $\{A \subseteq S \mid A \neq S\}$.

We first prove $\mathbb{N}$ is infinite. We define the set $A_1 \subset \mathbb{N}$ as follows:

$$A = \{n \in \mathbb{N} \mid 2n\}.$$

Note that A_1 is a proper subset of S because every element $a \in A_1$ also belongs to $\mathbb{N}$, but there is at least one element in $\mathbb{N}$ (in fact all odd natural numbers) that is not in A_1. With these sets defined, we have the function $f : A_1 \to \mathbb{N}$, i.e. $f(2n) = n$, for all $n \in \mathbb{N}$. To prove f is injective, we pick any two arbitrary elements $f(n_1) = f(n_2) \in \mathbb{N}$ and show that it must be the case that $n_1 = n_2 \in A_1$. $f(n_1) = f(n_2) \Leftrightarrow \frac{n_1}{\cancel{2}} = \frac{n_2}{\cancel{2}} \Leftrightarrow n_1 = n_2$. Therefore f injective, and we have proven $\mathbb{N}$ infinite.

We now prove $\mathbb{Z}$ is infinite. We define the set $A_2 \subset \mathbb{Z}$ as the set $\mathbb{N}$. Note that $\mathbb{N}$ is a proper subset of S because $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$; so every element $n \in \mathbb{N}$ also belongs to $\mathbb{Z}$, but there is at least one element in $\mathbb{Z}$ (in fact all non-positive integers) that is not in $\mathbb{N}$. Consider the function

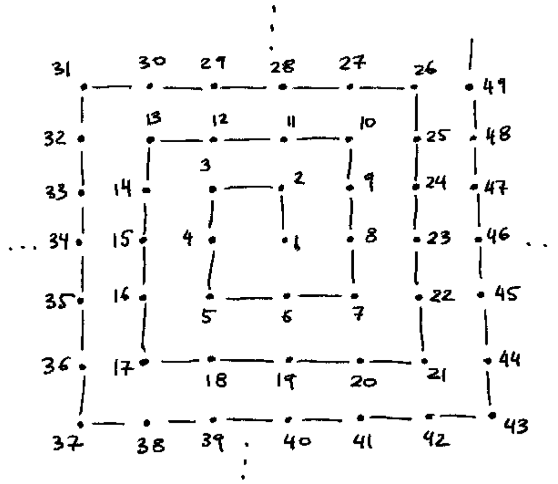

FIGURE 1. Mapping from $\mathbb{Q}$ to $\mathbb{N}$. Each point on the spiral represents an element $(a, b) \in \mathbb{Q}$ that is mapped to a natural number $n \in \mathbb{N}$.

$f : \mathbb{Z} \to \mathbb{N}$ defined by:

$$f(n) = \begin{cases} 2n+1 & \text{if } n \geq 0 \\ -2n & \text{if } n < 0 \end{cases}$$

for all $n \in \mathbb{N}$. Pick any two arbitrary $f(n_1) = f(n_2) \in \mathbb{N}$. If $f(n_1) = f(n_2)$ is odd, then $n_1 = n_2$ and is the nonnegative integer preimage that maps to the odd natural number $2n_1 + 1 = 2n_2 + 1 \Leftrightarrow n_1 = n_2$, else if $f(n_1) = f(n_2)$ is even then $n_1 = n_2$ and is negative. Therefore f is injective, and $\mathbb{Z}$ is infinite.

We now prove $\mathbb{Q}$ is infinite. We define the set $A_3 \subset \mathbb{Q}$ as the set of natural numbers $\mathbb{N}$. Note that $\mathbb{N}$ is a proper subset of $\mathbb{Q}$ because every element in $\mathbb{N}$ is an element of $\mathbb{Q}$ (in particular all elements with denominator 1) but there is at least one $q \in \mathbb{Q}$ (eg. $\frac{2}{3}$) that is not in $\mathbb{N}$. Consider the function $f : \mathbb{Q} \to \mathbb{N}$ defined as the mapping from elements $(a, b) = \frac{a}{b} \in \mathbb{Q}$ where $gcd(a, b) = 1$, for all $a, b \in \mathbb{Z}$. In Figure 1, imagine there are two coordinate axes pointing in the upwards and rightwards direction, corresponding to a and b respectively, i.e. the point $(1, 0) = \frac{1}{0}$ is represented by the point 1 as shown, even though the value might not necessarily be valid (which in this case it is not because the denominator is 0). But Figure 1 nonetheless proves that there exists an injection from $\mathbb{Q}$ to $\mathbb{N}$, because every simplest rational number (a, b) can be mapped to a natural number, and each natural number has only one rational number preimage. Therefore Q is infinite.

$\square$