Math 4317, Exam 1

1. (Assignment 1A Problem 9) Let E be any subset of the real numbers $\mathbb{R}$ and assume $u : E \to \mathbb{R}$ satisfies

$$u(x) \leq u(y) \text{ for all } x, y \in E \text{ with } x < y.$$

In this case, we say u is **monotone non-decreasing**.

(a) Let $x_0 \in \mathbb{R}$ be fixed. Show the set

$$V = \{u(x) : x \in E \text{ and } x > x_0\}$$

is **bounded below** but not necessarily **bounded above**. Note: To show V is **bounded below** you need to show there is a real number ℓ such that $\ell \leq v$ for every $v \in V$. To show V is *not necessarily* bounded above means to give an explicit example where V is not bounded above, i.e., there is no real number U such that $v \leq U$ for every $v \in V$. The number ℓ is called a **lower bound**. The number U, were such a number to exist, is called an **upper bound**.

(b) The completeness of the real numbers implies that a *nonempty* set of real numbers which is bounded below has a **greatest lower bound**, that is, a real number ℓ_0 which is a lower bound such that $\ell_0 \geq \ell$ for every lower bound ℓ. Does the set V from the previous part of this problem necessarily have a greatest lower bound? Note: If your answer is "yes," then you should prove it. If your answer is "no," then you should give an example, i.e., counterexample.

(c) If the set V from the first part of this problem has a greatest lower bound, show the set of lower bounds for V,

$$A = \{\ell : \ell \leq v \text{ for all } v \in V\},$$

is bounded above.

(d) If the set V from the first part of this problem has a greatest lower bound ℓ_0, show the least upper bound U_0 of the set A from the previous part satisfies $U_0 \leq \ell_0$.

Solution:

(a) The problem is incorrectly stated. If $E \cap \{x : x \leq x_0\} = \phi$, then it may be that the set V is neither bounded above nor below. For example, if $E = (0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$ with $x_0 = 0$ and $u(x) = 1/(1 - x) - 1/x$, then the set $V = \mathbb{R}$.

If, however, $E \cap \{x : x \leq x_0\}$ contains a point x_1, then $u(x_1) \leq u(x)$ for every $x \in E$ and the set V is bounded below.

Alternative solution: The professor meant "$x_0 \in E$" instead of "$x_0 \in \mathbb{R}$." If we know $x_0 \in E$, then for every $x \in E \cap (x_0, \infty) = \{x \in E : x > x_0\}$ we have $u(x_0) \leq u(x)$ by monotonicity. Therefore, $u(x_0)$ is a lower bound for V.

(b) The answer is "no" for a couple possible reasons. First of all, it could be that V is empty. Here is an example of that: $E = (-1, 0) = \{x : -1 < x < 0\}$ with $x_0 = 0$ and $u(x) \equiv 0$.

It could be that V is nonempty but the set V is not bounded below as in the (counter) example from the first part.

If, however, we have as suggested before $E \cap \{x : x \leq x_0\} \neq \phi$, then E is certainly bounded below. If we have, moreover, $E \cap \{x : x > x_0\} \neq \phi$, then V is nonempty and bounded below, so V will have a greatest lower bound.

Alternative solution: Assuming $x_0 \in E$, the answer to this part is (still) "no" because the set V, though bounded below, may be empty. As an example we can take

$$E = (-\infty, x_0] = \{x \in \mathbb{R} : x \leq x_0\} \text{ with } u : (-\infty, x_0] \to \mathbb{R} \text{ by } u(x) \equiv 1.$$

(c) If V has a greatest lower bound, this means V is nonempty and bounded below. In particuar, $E \cap \{x : x > x_0\} \neq \phi$. This means there is some $x_1 \in E \cap \{x : x > x_0\}$, and for every lower bound ℓ of V, we must have $\ell \leq u(x_1)$. This means the set

$$A = \{\ell : \ell \leq v \text{ for all } v \in V\}$$

is bounded above. We note, furthermore, that in this case, the greatest lower bound ℓ_0 of V, assumed to exist, has $\ell_0 \in A$. Thus A is nonempty.

Alternative solution: I don't see much alternative here. You need to use the fact that $V \neq \phi$ to get a point $x \in E \cap (x_0, \infty)$. Then A is bounded (above) because $\ell \leq u(x)$ for every $\ell \in A$.

(d) As mentioned in the previous part, $\ell_0 \in A$. Furthermore, ℓ_0 is the greatest lower bound of V. This means $\ell \leq \ell_0$ for all $\ell \in A$. Thus, ℓ_0 is an upper bound for A and $\ell_0 \in A$, which means ℓ_0 is the maximum element in A. Thus, not only is it the case that the least upper bound U_0 of A exists and satisfies $U_0 \leq \ell_0$, but ℓ_0 is the maximum of A and $\ell_0 = U_0$.

Alternative solution: Assuming $x_0 \in E$, we know from the previous part that $u(x_0)$ and ℓ_0 are both in A (though we may have $u(x_0) = \ell_0$ as, for example, when $E = [x_0, \infty) = \{x \in \mathbb{R} : x \geq x_0\}$ and $u : [x_0, \infty) \to \mathbb{R}$ by $u(x) \equiv 1$). In any case, we know $A \neq \phi$. As in the previous part, we also know $V \neq \phi$, and for every $v = u(x) \in V$, we have

$$\ell \leq v \qquad \text{for every } \ell \in A. \tag{1}$$

This means, on the one hand, that A is bounded above, so the least upper bound U_0 of A exists.

On the other hand, (1) also holds for any $v \in V$ which means every $\ell \in A$ is a lower bound for V. Therefore, $\ell \le \ell_0$ for every $\ell \in A$ because ℓ_0 is the greatest lower bound. This means ℓ_0 is an upper bound for A and hence $U_0 \le \ell_0$ because U_0 is the least upper bound of A.

Of course, as mentioned above, $\ell_0 \in A$, so we know $\ell_0 \le U_0$ as well. That is, $U_0 = \ell_0 = \max A$.

(e) Finally, it might be nice to give an example where $u(x_0) < \ell_0 = U_0$. This would be a discontinuity for u. We can take $E = [x_0, \infty) = \{x \in \mathbb{R} : x \ge x_0\}$ with

$$u(x) = \begin{cases} 0, & x = x_0 \\ 1, & x > x_0. \end{cases}$$

The first part of this problem offers you, the student, a number of opportunities for learning if you are able to take advantage of them. Some are easy and simple, and some are, apparently, very difficult for most people. Most of the important things to be learned here go well beyond the following very simple observations:

1. The empty set is bounded above and below.

2. Every **nonempty** set of real numbers which is bounded below has a greatest lower bound.

These observations, of course, play a role. In an effort to point out some much more important things, let me start with a traditional principle for taking math classes.

> *If the professor asks you to prove something that is true, then prove it.*
> *If the professor asks you to prove something that is not true, figure out what he meant or what is true, and prove that.*

If we can move beyond the "traditional" point of view, there are other things to learn. Nevertheless, this traditional statement contains a couple important points. First, it can be very difficult to compose a correct statement in mathematics. Even the professor can get it wrong, so:

> *It's dangerous to trust "authority," and doing so can blind you to things that are pretty obvious.*

It's probably even harder to compose a correct statement without mathematics—or about a subject that extends beyond mathematics—like anything in the real world.

The traditional statement also contains a certain element which says:

> *Nobody (even the professor) should take himself too seriously. Errors are to be expected, and that's okay.*

The traditional statement has also, I think, some shortcomings. First of all, the assumption that one can figure out the intention of the professor (or anyone else) is a bit shaky.

> *Ambiguity and error in human communication is the rule and not the exception.*

Furthermore, the presumption that one can figure out what is true, though a nice idea, should perhaps be tempered:

> *Humility and perspective are helpful doing mathematics. Again, there is no reason to take things so seriously. It's just a class. It's just a test.*

The lack of humility and perspective prevents most people, and even most mathematicians, from doing mathematics. We have the opportunity to learn some things and actually do some mathematics. Doing mathematics involves thinking about things carefully, not trusting anything, and trying to understand what's really going on. Having well-defined, correctly stated, "problems" and "exercises" can make people feel like they are doing mathematics, but ususally what they are doing is just, more or less blindly, "jumping through hoops." Jumping through hoops is not doing mathematics.

Mathematics is really a difficult psychological discipline which contradicts almost all of our conditioning as humans. We are conditioned to respect authority, to not think, and feel satisfied when things "work" but we do not really understand what is going on. It is really sad that most students and (mathematics) instructors think that the nice feeling of accomplishment from jumping through hoops is learning rather than the overwhelmed feeling of being confused, not understanding what is going on, and struggling to figure it out.

Having said that, I think there is a place for just "assuming" one understands something, and pushing on to other considerations. This allows one to set aside some (potentially confusing) details and consider other things which may make those details clearer. Getting bogged down in details is, at some point, to be avoided, and skipping details sometimes, rather than being indicative of a lack of humility, can offer an opportunity for even greater humility. This requires one to say: "I'm going to go on to try to understand what is going on over *here* based on the (false) assumption that I really understand what has gone on over *there*." As long as one keeps in mind his ignorance, and does not make too serious a blunder based on it, in particular, if one's mathematics is restricted to a psychological activity with very limited real world consequences, then hopefully one does not get in too much trouble.

And this brings me to my final observation concerning the role of humility in doing mathematics.

As I have said, it is sad that doing mathematics and taking mathematics courses is viewed by most people as "jumping through hoops," i.e., solving carefully composed and contrived problems and exercises. It is much worse when one views mathematics as a "means to change the world." This is what happens when one understands just enough to bring about certain significant changes and outcomes (especially in the real world) but does not fully understand what is going on and especially the consequences of those changes. As long as mathematics remains a psychological activity undertaken with adequte humility, then it doesn't seem to cause too much trouble. Probably the worst result is some wasted time, and that can be hard to avoid sometimes under any circumstances. Unfortuntely, it is all too common to confuse the mental gymnastics of mathematics with actual understanding of the real world which should be acted upon. In particular, to identify mathematical concepts with the physical world can be extremely dangerous. The classic example of this is the modification of the nuclei of atoms, as it is currently understood. Based on this we have nuclear bombs and so called nuclear "waste." We did not all want those things, but we all have them.

So here is a suggestion: If you think it's a good idea to impose anything on someone else based on your "understanding," especially your understanding of mathematics, then you probably don't have enough humility to do mathematics.

2. (intervals; Assignment 1A Problem 10) A set $I \subset \mathbb{R}$ is an **interval** if we have $x, y \in I$ with $x < y$, then we must have

$$[x, y] = \{\xi \in \mathbb{R} : x \leq \xi \leq y\} \subset I.$$

Show that every interval has exactly one of the following ten forms:

$$\begin{aligned}
&\phi \\
(-\infty, \infty) &= \mathbb{R} \\
(-\infty, b) &= \{x \in \mathbb{R} : x < b\} \\
(-\infty, b] &= \{x \in \mathbb{R} : x \leq b\} \\
(a, \infty) &= \{x \in \mathbb{R} : x > a\} \\
[a, \infty) &= \{x \in \mathbb{R} : x \geq a\} \\
(a, b) &= \{x \in \mathbb{R} : a < x < b\} \\
[a, b) &= \{x \in \mathbb{R} : a \leq x < b\} \\
(a, b] &= \{x \in \mathbb{R} : a < x \leq b\} \\
[a, b] &= \{x \in \mathbb{R} : a \leq x \leq b\}
\end{aligned}$$

Hint: Either an interval is bounded below—or it is not. They key is to find the numbers a and/or b.

Solution: First note that the empty set ϕ is an interval. For every pair of points $x < y$ in the empty set, one definitely has $[x, y] \subset \phi$. Thus, if I is an interval, one possibility is $I = \phi$.

In fact, each of the ten sets listed is an interval. This is obvious for $\mathbb{R}$. It is almost as obvious for the other eight sets. Take, for example, (a, b). If $x < y$ and $a < x < y < b$, then each $\xi \in [x, y]$ satisfies

$$a < x \leq \xi \leq y < b,$$

so $\xi \in (a, b)$. Thus, $[x, y] \subset (a, b)$, and we know (a, b) is an interval. If we consider $[a, b)$, then whenever $x < y$ with $a \leq x < y < b$, then each $\xi \in [x, y]$ satisfies

$$a \leq x \leq \xi \leq y < b.$$

Again, $[x, y] \subset [a, b)$ which shows that $[a, b)$ is an interval. The arguments showing the other six sets are intervals are very similar. It remains to show these are the only ten possibilities.

If I is not empty, then either I is bounded below, or it is not. Assuming, from here on, that I is not empty, let us consider the case that I is not bounded below.

Claim 1a: If I is not bounded below or above, then $I = \mathbb{R}$.

To see this, start with $x_0 \in I$. For any $x \in \mathbb{R}$ either $x < x_0$, $x = x_0$, or $x_0 < x$. This is because $\mathbb{R}$ is a totally ordered ring. In the first case, because I is not bounded below, there is some $x_1 \in I$ with $x_1 \leq x$. It follows that $x \in [x_1, x_0] \subset I$. If $x = x_0$, then clearly $x \in I$. If $x_0 < x$, then because I is not bounded above, there is some $x_1 \in I$ with $x_1 \geq x$. Thus, $x \in [x_0, x_1] \subset I$. We have shown that $x \in I$ for every $x \in \mathbb{R}$ and, hence, $I = \mathbb{R}$. The claim is established. $\square$

Claim 1b: If I is not bounded below but I is bounded above, then $I = (-\infty, b)$ or $I = (-\infty, b]$ where b is the least upper bound of I.

Since I is nonempty and bounded above, there is a well-defined least upper bound b. If $x \in I$, then $x \leq b$, since b is an upper bound for I. This means

$$I \subset (-\infty, b] = \{x \in \mathbb{R} : x \leq b\}.$$

If $b \in I$, then for any $x < b$, we know there is some $x_1 \leq x$ with $x_1 \in I$. This is because I is not bounded below. Then $x \in [x_1, b] \subset I$, and we have shown $(-\infty, b] \subset I$. Therefore, $I = (-\infty, b]$. If $b \notin I$, then for any $x < b$, we still know there is some $x_1 \leq x$ with $x_1 \in I$. Again, this is because I is not bounded below. On the other hand, there is some $x_2 \in I$ with $x \leq x_2 < b$. Otherwise, x would be an upper bound for I contradicting the fact that b is the **least** upper bound of I. Therefore, $x \in [x_1, x_2] \subset I$, and we have shown $(-\infty, b) \subset I$. Since $b \notin I$, we know also that $I \subset (-\infty, b)$, and the claim is established. $\square$

Thus, there are three possibilities when I is not bounded below and nonempty:

$$I = \mathbb{R}, \quad I = (-\infty, b), \quad \text{and} \quad I = (-\infty, b].$$

Similarly, there are three possibilities when I is nonempty and not bounded above. One of them is $I = \mathbb{R}$ of course. The other two possibilities occur when I is bounded below and are

$$I = (a, \infty) \quad \text{and} \quad I = [a, \infty)$$

where a is the greatest lower bound of I. The claims (say Claim 2a and Claim 2b) and proofs associated with these claims are very similar to those above.

We have six possibilites for I so far. Furthermore, we only need to consider the case when I is nonempty and bounded above and below. In this case, let a be the greatest lower bound of I and b the least upper bound of I. Clearly, if $x \in I$, then $x \leq b$ and $x \geq a$. This means $I \subset [a, b]$.

There are, of course, four remaining possibilities:

Claim 3a: If $a \in I$ and $b \in I$, then $I = [a, b]$.

Claim 3b: If $a \in I$ and $b \notin I$, then $I = [a, b)$.

Claim 3c: If $a \notin I$ and $b \in I$, then $I = (a, b]$.

Claim 3d: If $a \notin I$ and $b \notin I$, then $I = (a, b)$.

The proofs are similar. Take Claim 3b. If $x \in [a, b)$, then there is some $x_1 \in I$ with $x \leq x_1 < b$. Otherwise, x would be an upper bound for I contradicting that b is the **least** upper bound of I. By the property of intervals, we have $x \in [a, x_1] \subset I$. Thus, $[a, b) \subset I$. On the other hand, $b \notin I$, so $I \subset [a, b)$, and the claim is established. $\square$

For the next two problems below, assume $u : I \to \mathbb{R}$ is a monotone non-decreasing function defined on an interval I. You may use the following fact and definition: If the least upper bound U_0 of $u((-\infty, x_0))$ and the greatest lower bound ℓ_0 of $u((x_0, \infty))$ both exist, then

$$U_0 \leq u(x_0) \leq \ell_0. \tag{2}$$

Defintion If $x_0 \in I$ and *at least one* of the inequalities in (2) is strict, we say x_0 is a **point of discontinuity** of the monotone non-decreasing function u. Note: This definition does not require that both numbers U_0 and ℓ_0 exist.

3. (Assignment 1A Problem 12) Assume $u : I \to \mathbb{R}$ is a monotone non-decreasing function defined on an interval I.
   (a) If $x_0 \in I$, when is it possible that neither the least upper bound U_0 of $u((-\infty, x_0))$ nor the greatest lower bound ℓ_0 of $u((x_0, \infty))$ exist?
   (b) If $x_0 \in I$ is a point of discontinuity of u, what are the possible relations between U_0, ℓ_0, and $u(x_0)$?

Solution:

(a) If the set $(-\infty, x_0) \cap I$ is nonempty, then $u((-\infty, x_0)) \neq \phi$, and for every $v = u(x) \in (-\infty, x_0)$ we have $v = u(x) \leq u(x_0)$ by monotonicity. Thus, $u((-\infty, x_-))$ is a nonempty subset of $\mathbb{R}$ which is bounded above. The completeness of the real numbers then implies U_0 exists.

We conclude that if U_0 does not exist, then the set $(-\infty, x_0) \cap I$ is empty. In particular, this means

$$I \subset [x_0, \infty).$$

A very similar argument shows the following:

If ℓ_0 does not exist, then $I \subset (-\infty, x_0]$.

Combining these two observations, we conclude that the only situation in which neither U_0 nor ℓ_0 exist is when

$$I \subset (-\infty, x_0] \cap [x_0, \infty) = \{x_0\}.$$

Since we know $x_0 \in I$, this means $I = [x_0, x_0] = \{x_0\}$ must be a singleton if $x_0 \in I \neq \phi$, and in this case neither U_0 nor ℓ_0 exist. So, the answer is "yes." It is possible that neither U_0 nor ℓ_0 exist, and it happens precisely when I is a singleton. Furthermore,

If U_0 does not exist, then $I \subset [x_0, \infty)$,

and

if ℓ_0 does not exist, then $I \subset (-\infty, x_0]$.

(b) Here we are apparently assuming U_0 and ℓ_0 both exist which means, by the reasoning of the previous part, there are elements a and b in I with $a < x_0 < b$ (and of course $[a, b] \subset I$). We already know (or should know) that

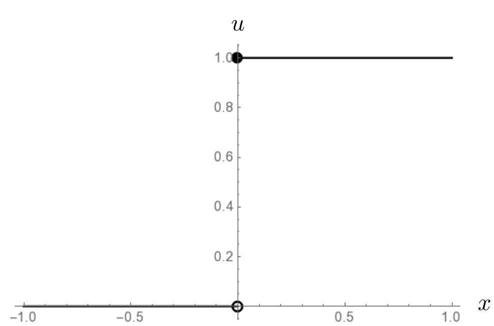
$$U_0 \leq u(x_0) \leq \ell_0 \tag{3}$$

and to have a discontiuity in this context means one of the inequalities in (3) is strict. Thus, nominally, there are three cases:

1. $U_0 < u(x_0) \leq \ell_0$,
2. $U_0 \leq u(x_0) < \ell_0$,
3. $U_0 < u(x_0) < \ell_0$.

We need to show by example that each of these three cases is non-vacuous. For each of the three examples, I will take $I = (-1, 1)$ and $x_0 = 0$.

1. If we set
$$u(x) = \chi_{[0,1)}(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0, \end{cases}$$
then $U_0 = 0 < u(x_0) = 1 = \ell_0$. Here is an illustration of the **graph** of this monotone function:

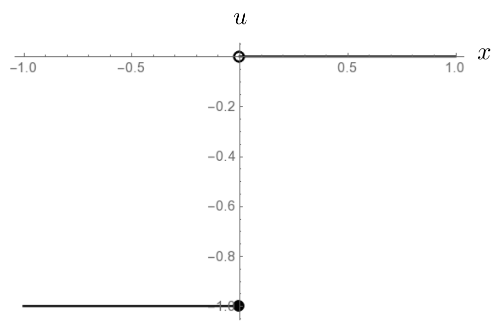


The graph is defined as the set $\{(x, u(x)) : x \in I\} \subset \mathbb{R}^2$.
In this case, $u((-\infty, x_0)) = u((-\infty, 0)) = \{0\}$ and $u((0, \infty)) = \{1\}$.

2. If we set

$$u(x) = -\chi_{(-1,0]}(x) = \begin{cases} -1, & x \leq 0 \\ 0, & x > 0, \end{cases}$$

then $U_0 = -1 = u(x_0) < 0 = \ell_0$. Here is an illustration of the graph of this monotone function:



In this case, $u((-\infty, x_0)) = u((-\infty, 0)) = \{-1\}$ and $u((0, \infty)) = \{0\}$.

3. Finally, if we set

$$u(x) = -\chi_{(-1,0)}(x) + \chi_{(0,1)}(x) = \begin{cases} -1, & x < 0 \\ 0, & x = 0, \\ 1, & x < 0, \end{cases}$$

we obtain a monotone non-decreasing function with

$$U_0 = -1 < 0 = u(x_0) < 1 = \ell_0.$$

In this case, $u((-\infty, x_0)) = \{-1\}$, $u((x_0, \infty)) = \{1\}$, and of course $u(x_0) = u(0) = 0$.

4. (Assignment 1A Problem 13) Assume $u : I \to \mathbb{R}$ is a monotone non-decreasing function defined on an interval I. Show the set of discontinuities of u is (at most) countable.

Solution: Let I_D denote the collection of discontinuities x_0 for which there exist real numbers $a, b \in I$ with $a < x_0 < b$. We can call these **interior** or **nice** discontinuities. We know that for these discontinuities $u((-\infty, x_0))$ is bounded above and nonempty and $u((x_0, \infty))$ is bounded below and nonempty. In particular, U_0 and ℓ_0 both exist for such a discontinuity and the definition of discontinuity gives us

$$U_0 < \ell_0. \tag{4}$$

Let I_E be the collection of all other discontinuities, i.e., discontinuities for which either U_0 does not exist or ℓ_0 does not exist. As we have seen in the previous problem, if $x_0 \in I_E$, then either

$$I \subset [x_0, \infty) \qquad \text{or} \qquad I \subset (-\infty, x_0].$$

We claim there can be at most two such discontinuties. In fact, there can be at most two such points in I period. If there were three such points $x_1, x_2, x_3 \in I_E$, then we would have (without loss of generality for the ordering)

$$x_1 < x_2 < x_3.$$

But this is an immediate contradiction because the definition of an interval tells us $[x_1, x_3] \subset I$, which means U_0 and ℓ_0 are well-defined real numbers for $x_0 = x_2$, and if there is a discontinuity at x_2, then $x_2 \in I_D$.

Thus, if we can show I_D is countable, then we know the collection of all discontinuities $I_D \cup I_E$ is countable. To show this, it is enough to obtain an injection $f : I_D \to \mathbb{Q}$ from the set of (interior) discontinuities into the rational numbers. Let $x \in I_D$ and let $U_0(x)$ be the least upper bound of $u((-\infty, x))$. Also, let $\ell_0(x)$ be the gretest lower bound of $u((x_0, \infty))$. Each interval $(U_0(x), \ell_0(x))$ is nonempty. Furthermore, because the real numbers is an Archimedean field, there is a rational number in every such interval. That is $(U_0(x), \ell_0(x)) \cap \mathbb{Q} \neq \phi$. Therefore, by the axiom of choice, there exists a function

$$f : I_D \to \bigcup_{x \in I_D} [(U_0(x), \ell_0(x)) \cap \mathbb{Q}] \text{ with } f(x) \in (U_0(x), \ell_0(x)) \cap \mathbb{Q} \text{ for every } x \in I_D.$$

We need only show that f is an injection. Assume $x_1, x_2 \in I_D$ with $x_1 < x_2$. Then

$$U_0(x_1) < f(x_1) < \ell_0(x_1) \qquad \text{and} \qquad U_0(x_2) < f(x_2) < \ell_0(x_2).$$

Consider $(x_1, x_2) \subset I$ and

$$x^* = (x_1 + x_2)/2 \in (x_1, x_2) = (-\infty, x_2) \cap (x_1, \infty)$$

in partiucular. Note that $\ell_0(x_1)$ is a lower bound for $u((x_1,\infty))$, and $U_0(x_2)$ is an upper bound for $u((-\infty,x_2))$. Therefore,

$$f(x_1) < \ell_0(x_1) \le u(x^*) \le U_0(x_2) < f(x_2).$$

This means $f(x_1) < f(x_2)$ and, in particular, $f(x_1) \ne f(x_2)$, so $f : I_D \to \mathbb{Q}$ is injective. $\square$

5. (Assignment 1B Problem 4) A function $\phi : G_1 \to G_2$ from one group G_1 to another G_2 is a **homomorphism** if $\phi(ab) = \phi(a)\phi(b)$ for every $a, b \in G_1$. A bijective homomorphism is called a group **isomorphism**, and two groups with a group isomorphism between them are said to be **isomorphic groups**.

   (a) Show that the **kernel**, $\ker(\phi) = \{a \in G_1 : \phi(a) = e\} = \phi^{-1}(e)$ where e is the identity element in G_2, of a homomorphism and the **image**, $\mathrm{im}(\phi) = \{\phi(a) : a \in G_1\} = \phi(G_1)$, of a homomorphism are subgroups of the groups G_1 and G_2 respectively.

   (b) If H is a subgroup of a group G, one can consider the **left cosets** of H given by

   $$aH = \{ah : h \in H\} \subset G$$

   and the **right cosets** $Ha = \{ha : h \in H\} \subset G$. A subgroup H is called **normal** if $aH = Ha$ for every $a \in G$. If H is a normal subgroup of G, then show the set of all (left) cosets $G/H = \{aH : a \in G\}$ with operation $(aH)(bH) = (ab)H$ is a group. This group G/H is called the **quotient group** of G by (the normal subgroup) H.

   (c) Show the kernel of a homomorphism is always a normal subgroup.

   (d) If $\phi : G_1 \to G_2$ is a homomorphism, then show $\mathrm{im}(\phi)$ and $G_1/\ker(\phi)$ are isomorphic groups. This is called the **first homomorphism theorem**.

Solution:

(a) In order to show a subset of a group, like $\ker(\phi) \subset G_1$, is a subgroup, I need to show the identity element is in the subset, the subset is closed under the operation, and the subset contains the inverse of each of its elements. Here is the verification for $\ker(\phi)$:

1. (identity element) Let e_1 denote the identity in G_1 and e_2 the identity in G_2. Let $b = \phi(e_1)$, and then we know there is an inverse element b^{-1} in G_2. Note that $\phi(e_1)\phi(e_1) = \phi(e_1 e_1) = \phi(e_1)$. Thus, multiplying by b^{-1} on both sides, we get
$$\phi(e_1) = bb^{-1} = e_2.$$
This means $e_1 \in \ker(\phi)$.

2. (closure) Consider $a, b \in \ker(\phi)$. Then we know $\phi(a) = e_2$ and $\phi(b) = e_2$. We want to show $ab \in \ker(\phi)$. In fact,

$$\phi(ab) = \phi(a)\phi(b) = e_2 e_2 = e_2.$$

This means $ab \in \ker(\phi)$.

3. (inverses) Consider $a \in \ker(\phi)$. Then $\phi(a) = e_2$. Also,

$$e_2 = \phi(e_1) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = e_2\phi(a^{-1}) = \phi(a^{-1}).$$

Thus, $\phi(a^{-1}) = e_2$, and $e_2 \in \ker(\phi)$.

We have shown $\ker(\phi)$ is a subgroup of G_1.

We next show $\mathrm{im}(\phi) = \{\phi(x) : a \in G_1\}$ is a subgroup of G_2.

1. (identity element) In fact, we have shown above that $\phi(e_1) = e_2$, so this means $e_2 \in \mathrm{im}(\phi)$.
2. (closure) Consider $\phi(a), \phi(b) \in \mathrm{im}(\phi)$. Then

$$\phi(a)\phi(b) = \phi(ab) \in \mathrm{im}(\phi).$$

3. (inverses) Consider $\phi(a) \in \mathrm{im}(\phi)$. Note that $\phi(a^{-1}) \in \mathrm{im}(\phi)$ as well. Also,

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_1) = e_2$$

and

$$\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(e_1) = e_2.$$

This means

$$[\phi(a)]^{-1} = \phi(a^{-1}) \in \mathrm{im}(\phi).$$

We have shown $\mathrm{im}(\phi)$ is a subgroup of G_2.

(b) 1. (well-defined operation) We will first show that the operation

$$(aH)(bH) = abH$$

on left cosets is well defined. Say $aH = \tilde{a}H$ and $bH = \tilde{b}H$. Then we need to show $abH = \tilde{a}\tilde{b}H$. Let $abh \in abH$ with $h \in H$. Since $bH = \tilde{b}H$, there is some $\tilde{h} \in H$ with $bh = \tilde{b}\tilde{h}$. Thus,

$$abh = a\tilde{b}\tilde{h}.$$

Since the group is normal, there is some $\hat{h} \in H$ such that $\tilde{b}\tilde{h} = \hat{h}\tilde{b}$. Thus,

$$abh = a\hat{h}\tilde{b}.$$

Since $aH = \tilde{a}H$, we have some $\check{h} \in H$ for which $a\hat{h} = \tilde{a}\check{h}$.

$$abh = \tilde{a}\check{h}\tilde{b}.$$

Finally, since H is a normal subgroup, we have $\check{h}\tilde{b} \in \tilde{b}\breve{h}$ for some smiling $\breve{h} \in H$, and

$$abh = \tilde{a}\tilde{b}\breve{h} \in \tilde{a}\tilde{b}H.$$

We hae shown $abH \subset \tilde{a}\tilde{b}H$. The reverse inclusion follows by an exchange of accents.

This means the operation is well-defined.

2. (associativity) In order for the cosets G/H to be a group, we need the operation to be associative. This follows almost immediately from the fact that the operation in G is associative:

$$(aH\, bH)cH = abH\, cH = (ab)cH = a(bc)H = aH\, bcH = aH(bH\, cH).$$

3. (identity) The identity in G/H is clearly $H = eH$ where e is the identity in G. In fact,

$$H\, aH = eH\, aH = eaH = aH = aeH = aH\, H.$$

4. (inverses) The inverses in G/H are equally obvious:

$$aH\, a^{-1}H = aa^{-1}H = eH = a^{-1}aH = a^{-1}H\, aH.$$

We have shown that G/H is a group.

(c) Here we want to show the kernel of a homomorphism $\phi : G_1 \to G_2$ is a normal subgroup of G_1. To see this, let $H = \ker(\phi)$ and consider aH. If $ah \in aH$, then we know $\phi(h) = e_2$ is the identity in G_2. Also, we can write

$$ah = aha^{-1}a$$

and

$$\phi(aha^{-1}) = \phi(a)\phi(h)\phi(a^{-1}) = \phi(a)e_2\phi(a^{-1}) = \phi(a)\phi(a^{-1}) = \phi(e_1) = e_2.$$

Therefore, $ah = \hat{h}a$ with $\hat{h} = aha^{-1} \in \ker(\phi) = H$. Thus, $aH \subset Ha$.

Similarly, if $ha \in Ha$, then $ha = aa^{-1}ha = a(a^{-1}ha) = a\hat{h}$ with $\hat{h} = a^{-1}ha$. It is clear that $\hat{h} \in \ker(\phi)$, so $ha \in aH$ and $Ha \subset aH$.

We have shown $H = \ker(\phi)$ is a normal subgroup in G_1.

(d) We need to find an isomorphism $\psi : G_1/\ker(\phi) \to \mathrm{im}(\phi)$. Let $H = \ker(\phi)$ as above and set $G = G_1$ and $I = \mathrm{im}(\phi)$. We define $\psi : G/H \to I$ by

$$\psi(aH) = \phi(a).$$

1. (well-defined) We need to show the function ψ is well-defined. If $aH = \tilde{a}H$, then there is some $h \in H = \ker(\phi)$ with $a = \tilde{a}h$. Therefore,

   $$\phi(a) = \phi(\tilde{a}h) = \phi(\tilde{a})\phi(h) = \phi(\tilde{a})e_2 = \phi(\tilde{a}).$$

   This shows ψ is well-defined.

2. (homomorphism) We need to show ψ is a group homomorphism.

   $$\psi(aHbH) = \phi(ab) = \phi(a)\phi(b) = \psi(aH)\psi(bH).$$

3. (injective) We need to show ψ is injective. If $\psi(aH) = \psi(bH)$, then

   $$\phi(a) = \phi(b). \tag{5}$$

   This means that if $ah \in aH$, then $ah = bb^1ah$. Now, we claim $\hat{h} = b^{-1}ah \in H$. In fact, using (5)

   $$\phi(b^{-1}ah) = \phi(b^{-1})\phi(a) = \phi(b^{-1})\phi(b) = \phi(e_1) = e_2.$$

   Therefore, $ah = b\hat{h} \in bH$, and we have shown $aH \subset bH$.

   The fact that $bH \subset aH$ now follows by exchanging the symbols a and b in the argument. Thus, $aH = bH$, and ψ is injective.

4. (surjective) It remains to show ψ is surjective, but this is immediate since given any $\phi(a) \in I = \mathrm{im}(\phi)$, we have

   $$\psi(aH) = \phi(a).$$