Math 127 Extra Credit Homework

Mary Radcliffe

The purpose of this set of problems is to prove that the real numbers exist; that is, that we can construct a complete ordered field, and that this construction is unique in a certain sense. Let us begin with what we shall assume.

We make the following assumptions to begin the construction.

- We know the integers and the rationals.
- We know that $\mathbb{Q}$ under the usual definition of addition and multiplication is a field.
- We know that $\mathbb{Q}$ under the usual definition of ordering is an ordered field.

We now begin with a construction of $\mathbb{R}$ from $\mathbb{Q}$.

Definition 1. Let $A \subseteq \mathbb{Q}$. We say that A is a *cut* if

1. If $x, y \in \mathbb{Q}$, with $x \in A$, and $y \leq x$, then $y \in A$.
2. A has an upper bound in $\mathbb{Q}$.
3. For every $x \in A$, there exists $y \in A$ such that $x < y$.

Let's first understand what this is.

Exercise 1. Prove that if A is a cut, and $r \notin A$, then $p < r$ for every $p \in A$.

So the idea with a cut is that we're literally slicing the rationals into two parts, a left side and a right side, and then we take the left side to be the set A. The place where we slice is what makes the cut special. In particular, we could choose to slice exactly at a rational:

Exercise 2. Prove that for any $q \in \mathbb{Q}$, there exists a cut A_q for which q is a least upper bound.

Exercise 3. Prove that if $p, q \in \mathbb{Q}$, with $p < q$, then $A_p \subset A_q$.

Excellent, so we can identify an element q of $\mathbb{Q}$ with a cut, by constructing a cut A_q that "ends" at q. And smaller elements of $\mathbb{Q}$ have strictly smaller cuts. But we can do even better! We can identify elements that aren't even in $\mathbb{Q}$ at all.

Exercise 4. Prove that $\{x \in \mathbb{Q} \mid x^2 \leq 2 \text{ or } x < 0\}$ is a cut.

Wow, neat, we were able to construct a cut whose slice is at $\sqrt{2}$. So what if we were able to use cuts to represent all the numbers? As we see above, when p, q are rational we can represent q with A_q, and $p < q$ gives us that $A_p \subset A_q$. But we have other cuts, like the one in Exercise 4, that represent irrational

numbers. So let's try to define a ordered field structure on the *cuts themselves*, allowing a cut to stand in for the number at which we slice the rationals. We begin with the ordering part.

Definition 2. Let $\mathcal{C} = \{A \subseteq \mathbb{Q} \mid A \text{ is a cut}\}$. Define an ordering on $\mathcal{C}$ by $A \leq B$ if and only if $A \subseteq B$.

Exercise 5. Prove that the ordering defined above is a total order; that is, it is a partial order, and any two elements of $\mathcal{C}$ are comparable.

Excellent, partway there. Now, to think about operations. In order to define a field structure, we need a 0 and 1, so we will take these elements as A_0 and A_1, as defined in Exercise 2. Note that by what we proved in Exercise 3, we have that $A_0 < A_1$, so $A_0 \neq A_1$. We'll start by defining addition.

Definition 3. Let $A, B \in \mathcal{C}$. Define $A + B = \{p + q \mid p \in A \text{ and } q \in B\}$.

Exercise 6. Prove the following are true about this definition of addition:

1. Closure: For all $A, B \in \mathcal{C}$, $A + B$ is a cut (so that when we add cuts, we stay within the universe of cuts).
2. Associativity: $A + (B + C) = (A + B) + C$ for all $A, B, C \in \mathcal{C}$
3. Identity: $A + A_0 = A$ for all $A \in \mathcal{C}$
4. Existence of inverses: For all $A \in \mathcal{C}$ there exists $B \in \mathcal{C}$ such that $A + B = A_0$. (Hint: set $B = \{p \in \mathbb{Q} \mid \exists r \notin A \text{ such that } p < -r\}$. Then prove that B is a cut, and $A + B = A_0$.)
5. Commutativity: For all $A, B \in \mathcal{C}$, $A + B = B + A$.
6. Order arithmetic: For all $A, B, C \in \mathcal{C}$, if $A \leq B$, then $A + C \leq B + C$.

Note: In the rest of this work, we shall refer to the set B constructed in part 4 above as $-A$. Just to check that this makes sense to us, and is consistent with how we think that addition should work in $\mathbb{Q}$:

Exercise 7. Let $p \in \mathbb{Q}$. Prove that $-A_p = A_{-p}$.

Neat, so we have now all the necessary properties for addition to make sense in our universe of cuts. It even plays well with the ordering we defined above! So the last thing we need in order to make sure this is an ordered field is a definition of multiplication. Warning: it's gonna look kinda weird. The reason that it looks weird is that when we do multiplication in the real numbers, something strange happens with negatives that we need to take care to account for with our cuts. Here's the problem. The cuts we're interested in are effectively left rays in $\mathbb{Q}$. We're taking all the rational numbers, down to $-\infty$, ending somewhere on the number line. But the problem is that if we had two negative numbers, when we multiply the values in their cuts together, we'll end up with a right ray in $\mathbb{Q}$, because the products of all those negatives become positives, and they go off to infinity. So we need to take especial care to ensure that when we do our products, we still end up with left rays, and they still represent what we want them to represent. So. Here we go.

Definition 4. Let $A, B \in \mathcal{C}$. If $A > A_0$ and $B > A_0$, define

$$A \cdot B = \{pq \in \mathbb{Q} \mid p \in A, q \in B, \text{ and } p, q \text{ are not both negative.}\}$$

Exercise 8. Prove that for $A, B > A_0$, the definition of $A \cdot B$ above yields a cut; that is, $A \cdot B \in \mathcal{C}$.

Exercise 9. Prove that if $p, q \in \mathbb{Q}$, and $p, q > 0$, then $A_p \cdot A_q = A_{pq}$.

Ok, good. So we have a definition of multiplication for positive numbers that makes sense. We'll define multiplication for negative numbers just by manipulation of the signs.

Definition 5. Let $A, B \in \mathcal{C}$. Define $A \cdot B$ as follows:

$$\begin{array}{ll} A \cdot B = A_0 & \text{if } A = A_0 \text{ or } B = A_0 \\ A \cdot B & \text{if } A > A_0, B > A_0 \\ -((-A) \cdot B) & \text{if } A < A_0, B > A_0 \\ -(A \cdot (-B)) & \text{if } A > A_0, B < A_0 \\ ((-A) \cdot (-B)) & \text{if } A < A_0, B < A_0 \end{array}$$

Whew, that's a lot of definition. And the bad news is that we still need to prove that this satisfies all the axioms for multiplication. That seems tough. So to facilitate that proof, let's get a little lemma first.

Exercise 10. For all $A, B \in \mathcal{C}$, prove that $-(A \cdot B) = (-A) \cdot B = A \cdot (-B)$.

(Note: You will need to consider cases, depending on the sign of A and B.)

Ok, so this exercise allows us to move negative signs through our products. That seems valuable for proving the other properties we care about for multiplication. For example, suppose we wanted to prove that multiplication is associative. First, we can start by looking at the case that A, B, C are all positive. In that case, we have

$$A \cdot (B \cdot C) \quad = \quad \{p(rs) \mid p \in A, r \in B, s \in C,\ p, rs \text{ not both negative, } r, s \text{ not both negative}\}$$

Note, if $p > 0$, then r can be negative or positive. If $p < 0$, then $rs > 0$, and since r, s are not both negative, it must be the case that $r > 0$. Hence, we have that p and r are not both negative. Moreover, if $pr < 0$, then one of p, r is negative. If it is p, then $r > 0$, and $rs > 0$, so $s > 0$. If it is r, then since r, s are not both negative, $s > 0$. In any case, we have that the condition listed above is equivalent to the condition that p, r are not both negative, and pr, s are not both negative; that is, $pr \in A \cdot B$ and $s \in C$. Thus, this is the same as taking $(A \cdot B) \cdot C$.

Hence, in the case that all three of A, B, C are positive, multiplication is associative. In the other cases, we may apply the result of Exercise 10:

If $A < 0, B > 0, C > 0$:

$$A \cdot (B \cdot C) = -((-A) \cdot (B \cdot C)) = -(((-A) \cdot B) \cdot C) = -(-(A \cdot B) \cdot C) = (A \cdot B) \cdot C.$$

If $A > 0, B < 0, C > 0$:

$$A \cdot (B \cdot C) = A \cdot (-((-B) \cdot C)) = -(A \cdot ((-B) \cdot C)) = -(A \cdot (-B)) \cdot C = (A \cdot B) \cdot C.$$

And so on. There are technically 8 cases to check, three of which are done here, but the other 5 are very similar.

The remaining properties can be checked in a similar way: first verify the property is true for positive cuts, and then extend that to negative cuts.

Exercise 11. Prove the following are true about this definition of multiplication:

1. Identity: $A \cdot A_1 = A$ for all $A \in \mathcal{C}$.
2. Inverse: For all $A \in \mathcal{C}$ with $A \neq A_0$, there exists $B \in \mathcal{C}$ such that $A \cdot B = A_1$. (Hint: set $B = \{p \in \mathbb{Q} \mid \exists r \notin A, p < \frac{1}{r}\}$ when $A > 0$.)
3. Commutativity: $A \cdot B = B \cdot A$ for all $A, B \in \mathcal{C}$.
4. Distributivity: $A \cdot (B + C) = A \cdot B + A \cdot C$ for all $A, B, C \in \mathcal{C}$.
5. Order arithmetic: For all $A, B \in \mathcal{C}$, if $A, B \geq A_0$ then $A \cdot B \geq A_0$.

Fantastic, things are going super well! Let's get a quick summary of what we've done up to this point.

- We defined a set $\mathcal{C}$.
- We endowed $\mathcal{C}$ with a linear order.
- We defined addition and multiplication in $\mathcal{C}$
- We proved that the order, addition, and multiplication satisfy all the axioms for an ordered field.

So, one thing left. We want to make sure that the ordered field we just made is complete. Recall, that means that for any subset of $\mathcal{C}$, there is a supremum for that set. Recall also that in $\mathcal{C}$, we have that the ordering is the same as in the power set lattice defined before: $A \leq B$ if and only if $A \subseteq B$. And, doubly good news, we already know how to take suprema in the power set lattice. Put those pieces together to solve the next exercise:

Exercise 12. Let $\mathcal{A} \subseteq \mathcal{C}$ be a set of cuts. Prove that there exists $S \in \mathcal{C}$ that satisfies the definition of a supremum.

So now, we have that $\mathcal{C}$ is not just an ordered field, it also has the property that every subset in $\mathcal{C}$ has a supremum. You've just proved the following theorem:

Theorem 1. *As defined here, $\mathcal{C}$ is a complete ordered field.*

In order to define the real numbers, then, we'll just say that $\mathcal{C}$ is them. We just stop using capital letters, and then, bam, real numbers. The rationals live inside this, hiding as what we've called A_q, and behave just like we expect. The behavior we get on all the other numbers is just an extension of what's going on in the rationals anyways.

One more point. Which we won't prove here. Let's get a real definition of what we mean by uniqueness. The theorem we would prove (which you can try, if you'd like) is as follows:

Theorem 2. *Let X be any complete ordered field. Then there exists a bijective function $f : X \to \mathcal{C}$ satisfying the following:*

1. *$x \leq_X y$ if and only if $f(x) \leq f(y)$ (that is, f doesn't change the ordering)*
2. *$f(x + y) = f(x) + f(y)$ (that is, f doesn't change the addition)*

3. $f(x \cdot y) = f(x) \cdot f(y)$ *(that is, f doesn't change the multiplication)*

So what's this here? We have a function between X and $\mathcal{C}$, it's bijective, and doing the function doesn't change any of the field or ordering structure? In what way, then, are X and $\mathcal{C}$ actually different? Answer: in no way at all. They're the same in every measurable way. So if you think you have a different complete ordered field, you don't really, because it must be the same as $\mathcal{C}$ in every way possible. This is what we mean by uniqueness.

The proof of this theorem is technical, and if you've gotten this far you've already done plenty of technical stuff. But basically, here's how the proof goes. First, show that any complete ordered field has to have $\mathbb{Q}$ as a subset. This is straightforward, since it will have to have $\mathbb{Z}$ as a subset (due to repeated addition of 1) and then will have to have all quotients in $\mathbb{Z}$ (hence $\mathbb{Q}$). This will instantly imply that $\mathbb{Q} \subseteq X$.

Then, take subsets in $\mathbb{Q}$. In particular, if you take subsets corresponding to cuts, the upper bounds must be members of X too. So it has to contain everything we defined in $\mathcal{C}$, and the addition and multiplication and ordering must satisfy all the same structure as in $\mathcal{C}$. This gives us an injection from $\mathcal{C}$ to X that satisfies the conditions in the theorem. We need only show that this injection is also surjective.

Once that is finished, we have that there is only one complete ordered field. In the whole universe. In all of mathematics. Just the one.

Cool.