

# MATH 425a: Problem Set 2

Qilin Ye

August 29, 2020

**Problem 1** (1.9). Let  $x = A \mid B, x' = A' \mid B'$  be cuts in  $\mathbb{Q}$ . We defined

$$x + x' = (A + A') \mid \text{the rest of } \mathbb{Q}.$$

- (1) Show that although  $B + B'$  is disjoint from  $A + A'$ , it may happen in degenerate cases that  $\mathbb{Q}$  is not the union of  $A + A'$  and  $B + B'$ .
- (2) Infer that the definition of  $x + x'$  as  $(A + A') \mid (B + B')$  would be incorrect.
- (3) Why did we not define  $x \cdot x' = (A \cdot A') \mid \text{rest of } \mathbb{Q}$ ?

**Solution.**

- (1) It turns out that sometimes  $(A + A') \cup (B + B')$  would be missing an element of  $\mathbb{Q}$ . Before we begin, define set  $\mathcal{S} = \{x \in \mathbb{Q} \mid x > 0 \text{ and } x^2 < 2\}$ , namely all positive rational numbers less than  $\sqrt{2}$  (note that we cannot actually use this definition because  $\sqrt{2}$  is not in  $\mathbb{Q}$ .) Now consider sets

$$\begin{aligned}x &= A \mid B = \{r \in \mathbb{Q} \mid r \leq 0 \text{ or } r \in \mathcal{S}\} \mid \text{the rest of } \mathbb{Q} \\x' &= A' \mid B' = \{r \in \mathbb{Q} \mid r \leq 0 \text{ or } r < 2 - s, \forall s \in \mathcal{S}\} \mid \text{the rest of } \mathbb{Q}\end{aligned}$$

Though I want to define the set  $A'$  as the set of all rational numbers less than  $2 - \sqrt{2}$ , but again we cannot say so because, again,  $2 - \sqrt{2}$  is not a rational number.

Having constructed the two sets without involving  $\mathbb{R}$ , hopefully now I may use  $\sqrt{2}$  now. Since  $a < \sqrt{2}$  for all  $a \in A$  and  $a' < 2 - \sqrt{2}$  for all  $a' \in A'$ , it follows that all elements of  $A' + B'$  are strictly less than  $\sqrt{2} + (2 - \sqrt{2}) = 2$ . Therefore  $2 \notin A + A'$ .

On the other hand, since  $\sqrt{2}$  is irrational,  $B = \{r \in \mathbb{Q} \mid r > 0 \text{ and } r^2 \geq 2\}$  is the same as  $\{r \in \mathbb{Q} \mid r > 0 \text{ and } r^2 > 2\}$ . In other words, all elements of  $B$  are strictly larger than  $\sqrt{2}$ . Likewise, all element of  $B'$  are strictly larger than  $2 - \sqrt{2}$ . Therefore, all elements of  $B + B'$  are strictly larger than  $\sqrt{2} + (2 - \sqrt{2}) = 2$ . Hence  $2 \notin B + B'$  either. Therefore  $(A + A') \cup (B + B')$  is not equal to  $\mathbb{Q}$ .

- (2) Based on the definition, if  $X \mid Y$  is a Dedekind cut then  $X \cup Y = \mathbb{Q}$  which is not the case for  $(A + A')$  and  $(B + B')$  as shown in (1).

- (3) We do not define multiplication as such because the product of two negative numbers is positive, and so  $(A \cdot A')$  can give us arbitrarily large positive numbers which we do not want.

**Problem 2** (1.10). Prove that for each cut  $x$  we have  $x + (-x) = 0^*$ . **This is not trivial.**

**Solution.** The proof involves the assumption that  $\mathbb{Q}$  has the Archimedean property. For clarity, we will denote  $0^* = A_0 \mid B_0$ ,  $x = A \mid B$ , and  $-x = A' \mid B'$ . The first case is when  $x = -x = 0^*$ . In this case  $A_0 = A = A'$  and the proposition  $x + (-x) = 0^*$  is trivial.

Now, if  $x, (-x) \neq 0$ , without loss of generality (WLOG) we may assume  $x > 0$ , i.e.,  $A_0 \not\subseteq A$ . To show  $x + (-x) = 0^*$  or  $A + A' = A_0$ , we need to show both  $(A + A') \subset A_0$  and  $(A + A') \supset A_0$ .

Showing  $\subset$  is easy. Since  $\forall b \in B$  and  $\forall a \in A$  we always have  $b > a$ . It follows that, for all  $a \in A$  and for all  $b \in B$  such that  $\exists c > 0$  and  $-b - c \notin A$  (i.e., for all elements of  $B$  excluding the smallest one — recall how  $A'$  of  $(-x)$  is defined),  $a + (-b) < 0$  always holds, i.e.,  $A + A' \subset A_0$ .

Now for the  $\supset$  part. First pick an arbitrary  $m = A_m \mid B_m$  satisfying  $A_m \not\subseteq A_0$ , i.e.,  $m < 0$ . Clearly  $m$  is negative. Now set  $n = -\frac{m}{2}$ , clearly a positive number.<sup>1</sup> Since  $\mathbb{Q}$  has the Archimedean property, there exists an integer  $k$  such that

$$\begin{cases} kn \in A, & \text{i.e., } kn < x \\ (k+1)n \in B, & \text{i.e., } (k+1)n \geq x \end{cases}$$

Now let  $j = -(k+2)n$ . Recall the definition of  $-x$  when  $x = A \mid B$ :

$$-x = C \mid D = \{r \in \mathbb{Q} \mid \text{for some } b \in B, \text{ not the smallest element of } B, r = -b\} \mid \text{the rest of } \mathbb{Q}$$

If we look at  $-j = (k+2)n$ , we know  $-j > (k+1)n$  since  $n$  is positive. Therefore  $-j$  is not the smallest element of  $B$  and thus  $j \in A'$ . Now we have  $kn \in A$  and  $j \in A'$ . Adding them together gives

$$kn + j = kn - (k+2)n = -2n = m.$$

Therefore any arbitrary  $a_0 \in A_0$  can be written as the sum of some  $a \in A$  and  $a' \in A'$ . We have  $(A + A') \supset A_0$ .

Having shown  $(A + A') \subset A_0$  and  $(A + A') \supset A_0$ , we conclude that  $(A + A') = A_0$  and thus  $x + (-x) = 0^*$ . Really not trivial... □

**Problem 3** (1.12). Prove that there exists no smallest positive real number. Does there exist a smallest positive rational number? Give a real number  $x$ , does there exist a smallest real number  $y > x$ ?

**Solution.** All answers are NO.

<sup>1</sup>Rudin W. *Principles of Analysis*. 3<sup>rd</sup> ed., McGraw-Hill, 1976, p.19.

- (1) Suppose  $x > 0$  is the smallest positive real number. Since we know  $1 > \frac{1}{2}$ , it follows that  $1 \cdot x > \frac{1}{2} \cdot x \implies x > \frac{x}{2}$ , and we've just found a smaller positive real number. Contradiction. Therefore there does not exist a smallest positive real number.
- (2) Similar to (1) except the word "real" is replaced by "rational".
- (3) Suppose no, then the statement implies there is no real number  $x$  such that  $x > 0$  and  $x < y - x$ . Otherwise we can simply add the smaller number to  $x$  and find a real number greater than  $x$  but smaller than  $y$ . By (1) we are always able to come up with such numbers. Therefore, given  $x$ , there does not exist a smallest real number  $y > x$ .

**Problem 4** (1.14). Prove that  $\sqrt{2} \in \mathbb{R}$  by showing that  $x \cdot x = 2$  where  $x = A | B$  is the cut in  $\mathbb{Q}$  with  $A = \{r \in \mathbb{Q} \mid r \geq 0 \text{ or } r^2 < 2\}$ .

**Solution.** Recall that the definition of  $x \cdot x$  where  $x = A | B$  is

$$x \cdot x = C | D = \{r \in \mathbb{Q} \mid r \leq 0 \text{ or } \exists \text{ positive } a, b \in A \text{ such that } r = ab\} \mid \text{the rest of } \mathbb{Q}.$$

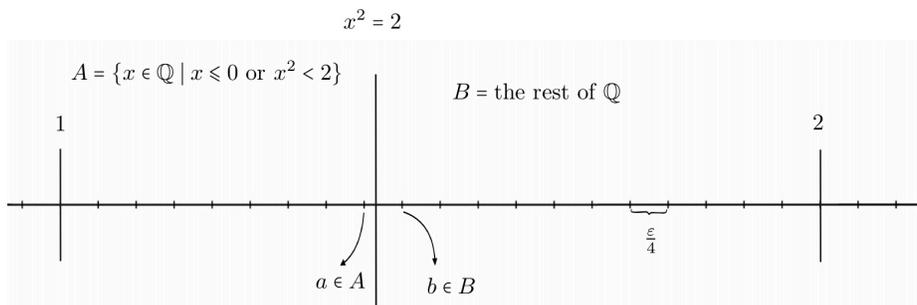
Also note that  $2 = E | F = \{x \in \mathbb{Q} \mid x < 2\} \mid \{x \in \mathbb{Q} \mid x \geq 2\}$ . To show  $x \cdot x = 2$ , we have to show  $(C \subset E) \wedge (C \supset E)$  so that  $C = E$ .

Like the first problem, showing  $\subset$  is super easy: if  $a, b$  satisfy  $a^2, b^2 < 2$ , then  $ab < 2$ . Therefore  $C \subset E$ .  
 On the other hand, we want to show  $E \subset F$ . A formal way to phrase this statement is the following:

For each  $\epsilon > 0$ , there exists  $a \in A$  such that  $2 - \epsilon < a^2 < 2$ .

In other words, if  $2 - \epsilon = c \in C$  then there exists  $a^2 \in E$  such that  $a^2 > c$  so  $c \in E$  as well.

Now imagine 1, 2 sitting on an evenly spaced axis of rational numbers. We may divide the interval between 1 and 2 into many sub-intervals, each with length  $\epsilon/4$ . Again, by the Archimedean property of  $\mathbb{Q}$ , among all the endpoints of these sub-intervals, there exists an adjacent pair, where the square of the value of the left one  $< 2$  and the other  $> 2$ . To visualize this, see the not-to-scale diagram below.



Since  $a < 2$  and  $b < 2$ , we know  $a + b < 4$ . Moreover, we also know  $b - a = \epsilon/4$ . Therefore  $b^2 - a^2 = (b + a)(b - a) < \epsilon$ . Since  $b^2 > 2$  and  $a^2 < 2$ , we know that the point 2 is between  $a$  and  $b$ . Therefore  $2 - a^2 < b^2 - a^2 < \epsilon$ , and we've successfully found an  $a$  such that  $2 - \epsilon < a^2 < 2$ . Hence  $C \supset E$  and therefore  $C = E$ ,  $x \cdot x = 2$ .  $\square$

**Problem 5** (1.15). Given  $y \in \mathbb{R}$ ,  $n \in \mathbb{N}$ , and  $\epsilon > 0$ , show that for some  $\delta > 0$ , if  $u \in \mathbb{R}$  and  $|u - y| < \delta$  then  $|u^n - y^n| < \epsilon$ . Hint: use induction and consider the identity

$$u^n - y^n = (u - y)(u^{n-1} + u^{n-2}y + \cdots + y^{n-1}).$$

**Solution.** I managed to finish this problem without induction. Here is my claim:

Given  $y \in \mathbb{R}$ ,  $n \in \mathbb{N}$ , and  $\epsilon > 0$ , if  $\delta < \min\left(1, \frac{\epsilon}{n(|y| + 1)^{n-1}}\right)$ , then if  $u \in \mathbb{R}$ ,  $|u - y| < \delta \implies |u^n - y^n| < \epsilon$ .

*Proof.* For convenience, we prefer to limit  $\delta < 1$  using a  $\min()$  function when necessary.<sup>2</sup>

If  $|u - y| < 1$ , then  $|u| < |y| + 1$  and  $|y| < |y| + 1$ . It follows that

$$\begin{aligned} |u^n - y^n| &\leq |u - y| \left| \sum_{i=0}^{n-1} y^i u^{(n-1)-i} \right| && \text{(by the identity given in question)} \\ &\leq |u - y| \sum_{i=0}^{n-1} |y^i u^{(n-1)-i}| && \text{(iterations of triangle inequality)} \\ &< |u - y| \sum_{i=0}^{n-1} (|y| + 1)^{n-1} && \text{(assumption that } |y| < |y| + 1) \\ &< \delta(n)(|y| + 1)^{n-1}. \end{aligned}$$

Therefore if we set  $\delta < \min\left(1, \frac{\epsilon}{n(|y| + 1)^{n-1}}\right)$  then

$$|u^n - y^n| < \frac{\epsilon}{n(|y| + 1)^{n-1}} (n)(|y| + 1)^{n-1} = \epsilon$$

from which we conclude that the claim holds.  $\square$

**Alternate Solution 1.** This time we will actually use (strong)<sup>3</sup> induction as suggested by the hint. Let  $\varphi(n)$  be the statement

Given  $y \in \mathbb{R}$ ,  $n \in \mathbb{N}$ ,  $\epsilon > 0$ , there exists  $\delta > 0$  such that if  $u \in \mathbb{R}$  and  $|u - y| < \delta$  then  $|u^k - y^k| < \epsilon$  for all integers  $k \in [0, n]$ .

<sup>2</sup>Idea came a casual chat with Prof. Andrew Manion during his office hours.

<sup>3</sup>Linfeng suggested that I try strong induction as opposed to weak induction, and he gave me hints on how to set up  $\varphi(n)$ .

Furthermore,  $\delta$  can be defined as

$$\delta < \begin{cases} \min\left(\frac{\epsilon}{2n|y|^{n-1}}, \frac{1}{2n|y|^{n-1}}\right), |y| \geq 1 \\ \min\left(\frac{\epsilon}{2n|y|^{n-1}}, \frac{1}{2n|y|}\right), |y| < 1. \end{cases}$$

Clearly  $\varphi(1)$  is trivial. To see  $\varphi(2)$  is true, consider the following:

$$\begin{aligned} |u^2 - y^2| &\leq |u - y||u + y| \\ &= |u - y| \left| \sum_{i=0}^1 y^i u^{1-i} \right| && \text{(just written in another form)} \\ &\leq |u - y| \sum_{i=0}^1 |y^i| |u^{1-i}| \\ &\leq |u - y| \sum_{i=0}^1 [|y^i| (|y^{1-i}| + |u^{1-i} - y^{1-i}|)] && \text{(triangle inequality)} \\ &< |u - y| \sum_{i=0}^1 [|y^i| (|y^{1-i}| + \epsilon)] && \text{(by the assumption that } |u^k - y^k| < \epsilon \text{ for all } k \in [0, 2]) \\ &\leq |u - y| \sum_{i=0}^1 (|y| + \epsilon |y^i|) \\ &\leq |u - y| (2|y| + 2\epsilon|y|) < \delta (2|y| + 2\epsilon|y|). \end{aligned}$$

Honestly, the case for  $n = 2$  could have been a lot simpler. However I deliberately did so just to illustrate that the definition of  $\delta$  above works. If  $n = 2$  then

$$\delta < \min\left(\frac{\epsilon}{4|y|}, \frac{1}{4|y|}\right) \text{ regardless of the magnitude of } y.$$

Substituting these values into the equation we see

$$\begin{aligned} \text{If } \frac{\epsilon}{4|y|} < \frac{1}{4|y|}, \text{ then } |u^2 - y^2| &< \frac{\epsilon}{4|y|} (2|y|) + \frac{\epsilon}{4|y|} (2\epsilon|y|) < \frac{\epsilon}{4|y|} (2|y|) + \frac{1}{4|y|} (2\epsilon|y|) = \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \text{ and} \\ \text{If } \frac{1}{4|y|} \leq \frac{\epsilon}{4|y|}, \text{ then } |u^2 - y^2| &< \frac{1}{4|y|} (2|y|) + \frac{1}{4|y|} (2\epsilon|y|) \leq \frac{1}{4|y|} (2|y|) + \frac{\epsilon}{4|y|} (2\epsilon|y|) = \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon. \end{aligned}$$

Hence  $\varphi(2)$  is also true. Now assume  $\varphi(k)$  is true, and we expand  $|u^{k+1} - y^{k+1}|$  below to show  $\varphi(k+1)$  also holds:

$$\begin{aligned}
 |u^{k+1} - y^{k+1}| &= \left| (u - y) \left( \sum_{i=0}^k y^i u^{k-i} \right) \right| && \text{(by the provided identity)} \\
 &\leq |u - y| \sum_{i=0}^k [|y^i| |u^{k-i}|] \\
 &\leq |u - y| \sum_{i=0}^k [|y^i| (|y^{k-i}| + |u^{k-i} - y^{k-i}|)] && \text{(triangle inequality)} \\
 &< |u - y| \sum_{i=0}^k [|y^k| + \epsilon |y^i|] && \text{(induction hypothesis, all } |u^i - y^i| < \epsilon) \\
 &\leq |u - y| \left( \sum_{i=0}^k |y|^n + \sum_{i=0}^k \max(|y|, |y|^k) \cdot \epsilon \right) && \text{(maximizing } \sum_{i=0}^k \epsilon |y^i|) \\
 &= \delta(k+1)|y|^k + \delta\epsilon(k+1) \max(|y|, |y|^k)
 \end{aligned}$$

Note that since we don't know if  $|y| \geq 1$ , we don't know if  $|y|$  or  $|y|^k$  is the largest element in the sequence  $|y|, |y|^2, \dots, |y|^k$ . Therefore we have to use a  $\max()$  function to determine so. Since the formula for  $\delta$  is highly similar in both cases, we will only verify the former here. Suppose  $|y| \geq 1$ ,  $n = k + 1$ , and we take

$$\delta < \min \left( \frac{\epsilon}{2(k+1)|y|^k}, \frac{1}{2(k+1)|y|^k} \right).$$

If  $\frac{\epsilon}{2(k+1)|y|^k} < \frac{1}{2(k+1)|y|^k}$ , then

$$|u^{k+1} - y^{k+1}| < \frac{\epsilon}{2(k+1)|y|^k} (k+1)|y|^k + \frac{\epsilon}{2(k+1)|y|^k} \epsilon(k+1)|y|^k < \frac{\epsilon}{2} + \frac{1}{2(k+1)|y|^k} \epsilon(k+1)|y|^k = \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon,$$

and if  $\frac{1}{2(k+1)|y|^k} \leq \frac{\epsilon}{2(k+1)|y|^k}$ , then

$$|u^{k+1} - y^{k+1}| < \frac{1}{2(k+1)|y|^k} (k+1)|y|^k + \frac{1}{2(k+1)|y|^k} \epsilon(k+1)|y|^k \leq \frac{\epsilon}{2(k+1)|y|^k} (k+1)|y|^k + \frac{\epsilon}{2} = \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Therefore we've shown  $\varphi(k) \implies \varphi(k+1)$ .

Having completed the base cases and the inductive step, we claim  $\varphi(n)$  holds for all  $n \in \mathbb{N}$ . □

**Alternate Solution 2.** Another solution uses weak induction but doesn't use the identity provided. However it's much less complicated. Before coming up with this solution, I was wondering if it's possible to express the degree  $n + 1$  function  $|u^{n+1} - y^{n+1}|$  by only using degree 1 and degree  $n$  functions — specifically  $|u^n - y^n|$ . The answer turns out to be very elegant:

$$\begin{aligned}
 |u^{n+1} - y^{n+1}| &\leq |u^{n+1} - uy^n| + |uy^n - y^{n+1}| \\
 &\leq |u||u^n - y^n| + |y^n||u - y|
 \end{aligned} \tag{1}$$

Similar to what we've done in the first proof, we may well keep  $|u - y| < 1$  using a  $\min()$  function so  $|u| < |y| + 1$ . Let  $\varphi(n)$  be the statement that

$$\text{Given } y \in \mathbb{R}, n \in \mathbb{N}, \text{ and } \epsilon > 0, \text{ there exists } \delta > 0 \text{ such that if } u \in \mathbb{R}, |u - y| < \delta \implies |u^n - y^n| < \epsilon.$$

Again  $\varphi(1)$  is trivial. To show  $\varphi(2)$  holds:

$$\begin{aligned} |u^2 - y^2| &\leq |u^2 - uy| + |uy - y^2| \\ &\leq |u||u - y| + |y||u - y| \\ &\leq (|y| + 1)|u - y| + |y||u - y| \\ &< \delta(2|y| + 1) \end{aligned}$$

Therefore if we set  $\delta < \min\left(1, \frac{\epsilon}{2|y| + 1}\right)$  then  $|u^2 - y^2| < \frac{\epsilon}{2|y| + 1}(2|y| + 1) = \epsilon$ . Now, for the inductive step, if we assume  $\varphi(k)$  to be true, then there exists  $\delta_k$  such that if  $|u - y| < \delta_k$  then  $|u^k - y^k| < \frac{\epsilon}{2(|y| + 1)}$ . (This fraction is particularly useful because we've set  $|u| \leq |y| + 1$  and the  $(|y| + 1)$  would cancel each other out during multiplication, leaving us with a neat  $\epsilon/2$ .) If we let

$$\delta_{k+1} < \min\left(1, \delta_k, \frac{\epsilon}{2(|y|^{k+1} + 1)}\right)^\dagger$$

<sup>†</sup>2 to create  $\epsilon/2$ ,  $|y|^k$  to cancel out  $|y^k|$  in inequality (1), +1 to avoid zero denominator.

then

$$\begin{aligned} |u^{k+1} - y^{k+1}| &\leq |u||u^k - y^k| + |y^k||u - y| && \text{(by the inequality (1) above)} \\ &< (|y| + 1) \underbrace{\frac{\epsilon}{2(|y| + 1)}}_{< |u^k - y^k| \text{ by hypothesis}} + (|y|^k + 1) \underbrace{\frac{\epsilon}{2(|y|^k + 1)}}_{\text{(by the construction of } \delta_{k+1})} \\ &= \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon. \end{aligned}$$

Therefore  $\varphi(k) \implies \varphi(k + 1)$  and the induction is done. Hence question proven.  $\square$

**Problem 6** (1.16). Given  $x > 0$  and  $n \in \mathbb{N}$ , prove that there is a unique  $y > 0$  such that  $y^n = x$ . That is, the  $n^{\text{th}}$  root of  $x$  exists and is unique. Hint: consider  $y = \sup(\mathcal{S})$  where  $\mathcal{S} := \{s \in \mathbb{R} \mid s^n \leq x\}$  and then show that  $y^n$  can neither  $< x$  or  $> x$ .

**Solution.** As suggested by the hint, the proof of existence divides into two parts. We first suppose, by contradiction, that  $y^n < x$ , and we pick  $\epsilon < x - y^n$  (so  $y^n + \epsilon < x$ ). Now, by the conclusion of the previous problem, we know that

$$\delta < \frac{\epsilon}{n(y + 1)^{n-1}} \implies (y + \delta)^n - y^n < \epsilon.$$

Therefore

$$(y + \delta)^n < y^n + \epsilon < x$$

from which we can immediately tell that  $y + \delta \in \mathcal{S}$ . Therefore  $y$  cannot be  $\sup(\mathcal{S})$  because it's not even an upper bound of  $\mathcal{S}$ .

Now for the other part, suppose  $y^n > x$  and we pick  $\epsilon < y^n - x$  (so that  $y^n - \epsilon > x$ ). Similarly, by the conclusion of the previous problem, we have

$$\delta < \frac{\epsilon}{n(y+1)^{n-1}} \implies y^n - (y-\delta)^n < \epsilon.$$

Therefore

$$(y-\delta)^n > y^n - \epsilon > x$$

from which the existence of  $y-\delta$  shows  $y$  is not the L.U.B. of  $\mathcal{S}$ . Hence it's impossible that  $y^n > x$ .

By trichotomy,  $y^n \not< x$  and  $y^n \not> x$  implies  $y^n = x$ .

Now we try to prove the uniqueness of such  $y$ . Two proofs below, both suppose that  $y' \in \mathbb{R}$  and  $(y')^n = x$ .

*First proof.* Clearly  $y'$  is also an upper bound of  $\mathcal{S}$ . It's also clear that  $y'$  is the L.U.B. because for any  $z \in \mathbb{R}$ ,  $z < y' \implies z^n < x$  and thus  $z$  cannot be an upper bound of  $\mathcal{S}$  as shown above. By trichotomy exactly one among  $y < y', y = y', y > y'$  is true. If  $y < y'$  then  $y'$  isn't the *least* upper bound, whereas if  $y > y'$  then  $y$  isn't the *least* upper bound. Therefore the only possibility is if  $y = y'$ . Hence proven.  $\square$

*Second proof.* We will first need a lemma.

**Lemma.** If  $0 < a < b$ , then  $a^n < b^n$  for all  $n \in \mathbb{Z}^+$ .

*Proof of lemma.* Suppose  $0 < a < b$ . Let  $\varphi(n)$  be the statement that  $a^n < b^n$ . Clearly  $\varphi(1)$  is true. Now suppose  $\varphi(k)$  holds, i.e.,  $a^k < b^k$ . Then since  $\mathbb{R}$  is a well-ordered field, we have  $a^{k+1} < b \cdot a^{k+1} < b^{k+1}$ .  $\square$

Back to the question. By trichotomy, if  $y' \neq y$ , then either  $y < y'$  or  $y' < y$ , and either  $x = y^n < (y')^n$  or  $(y')^n < y^n = x$ . Therefore if  $(y')^n = x$  then  $y' = y$ , i.e.,  $y$  is unique.  $\square$