MATH 327 Homework 1

Jaiden Atterbury

2024-04-02

Exercise 1. Given $(F, +, \cdot)$ a commutative field.

1. Prove that the additive inverse of any element of F is unique.

Proof: (Proof by contradiction) Let $a \in F$. Assume for the sake of contradiction that the additive inverse of a is not unique. Using the fact that $(F, +, \cdot)$ is a commutative field and thus each element a has an additive inverse, as well as the fact that we are assuming this additive inverse is not unique, we can let $(-a)_1$ and $(-a)_2$ be two different additive inverses of a. This implies that $a + (-a)_1 = 0$ and $a + (-a)_2 = 0$, where 0 is the unique additive identity of F (as proven in lecture). Thus it follows that

$$\begin{aligned}
(-a)_1 &= (-a)_1 + 0 \quad \text{(definition of an additive identity)} \\
&= (-a)_1 + (a + (-a)_2) \quad \text{(since } a + (-a)_2 = 0\text{)} \\
&= ((-a)_1 + a) + (-a)_2 \quad \text{(associative property of fields)} \\
&= (a + (-a)_1) + (-a)_2 \quad \text{(commutative property of fields)} \\
&= 0 + (-a)_2 \quad \text{(since } a + (-a)_1 = 0\text{)} \\
&= (-a)_2 \quad \text{(definition of an additive identity)}
\end{aligned}$$

Therefore, under the assumption that the additive inverse of a was not unique, we have shown that any two additive inverses of a are, in fact, equivalent in value. This contradiction shows us that the additive inverse of any element of F is unique. □

2. Prove that $(a * b)^{-1} = a^{-1} * b^{-1}$ for any two elements of F such that $a \neq 0$ and $b \neq 0$.

Proof: Let $a, b \in F$ such that $a \neq 0$ and $b \neq 0$. Since $a \neq 0$, by the definition of a multiplicative inverse, $\exists a^{-1} \in F$ such that $a * a^{-1} = 1$, where 1 is the multiplicative identity. By the same reasoning, for the element b, $\exists b^{-1} \in F$ such that $b * b^{-1} = 1$. Furthermore, since $a \neq 0$ and $b \neq 0$, it follows that $a * b \neq 0$, due to the first theorem proved in the appendix. Since $ab \neq 0$, it follows that $\exists (a * b)^{-1} \in F$ such that $(a * b) * (a * b)^{-1} = 1$.

From here, we will observe the term $(a * b) * (a^{-1} * b^{-1})$. Namely, we see that

$$\begin{aligned}
(a * b) * (a^{-1} * b^{-1}) &= (b * a) * (a^{-1} * b^{-1}) \quad \text{(commutative property of fields)} \\
&= b * (a * a^{-1}) * b^{-1} \quad \text{(associative property of fields)} \\
&= b * (1) * b^{-1} \quad \text{(definition of multiplicative inverse)} \\
&= b * b^{-1} \quad \text{(definition of multiplicative identity)} \\
&= 1 \quad \text{(definition of multiplicative inverse)}
\end{aligned}$$

Thus we have shown that $(a * b) * (a^{-1} * b^{-1}) = 1$. This means that $a^{-1} * b^{-1}$ is the multiplicative inverse of $a * b$, which is defined as $(a * b)^{-1}$. Hence we have shown that $(a * b)^{-1} = a^{-1} * b^{-1}$, given that $a \neq 0$ and $b \neq 0$. □

3. Prove that $(b^{-1})^{-1} = b$ for any element of F, $b \neq 0$.

Proof: Let $b \in F$ such that $b \neq 0$. Since $b \neq 0$, by the definition of a multiplicative inverse, $\exists b^{-1} \in F$ such that $b * b^{-1} = 1$, where 1 is the multiplicative identity. Furthermore, since $b \neq 0$ and $b * b^{-1} \neq 0$, by the second theorem proved in the appendix, it follows that $b^{-1} \neq 0$. Again, since $b^{-1} \neq 0$, by the definition of a multiplicative inverse, $\exists (b^{-1})^{-1} \in F$ such that $b^{-1} * (b^{-1})^{-1} = 1$. Multiplying b on both sides of this equality, we obtain $b * b^{-1} * (b^{-1})^{-1} = b$. By the associative property of fields, we can rewrite this expression as $(b * b^{-1})(b^{-1})^{-1} = b$. By the definition of a multiplicative inverse, we have $1 * (b^{-1})^{-1} = b$. By the definition of the multiplicative identity we have that $(b^{-1})^{-1} = b$. Thus, we have shown that, for any element b in F such that $b \neq 0$, $(b^{-1})^{-1} = b$. $\square$

Exercise 2. Let $\mathbb{R}$ be the set of real numbers. $+$ and $\cdot$ are the standard addition and multiplication for real numbers. For any real numbers x and y, we define $\oplus$ by

$$x \oplus y = x + y - 1$$

and $\otimes$ by

$$x \otimes y = x + y - xy$$

Is $(\mathbb{R}, \oplus, \otimes)$ a commutative field? You may use that $(\mathbb{R}, +, \cdot)$ is a commutative field, i.e. $+$, $\cdot$ are associative, commutative, distributive, 0 is the additive identity for $+$, 1 is the multiplicative identity for $\cdot$, etc.

Proof: In order to show that $(\mathbb{R}, \oplus, \otimes)$ is a commutative field, we must show that this algebraic structure satisfies the ten properties of fields. These properties include: closure, associativity, commutativity, distributivity, existence of the additive identity, existence of the multiplicative identity, existence of the additive inverse, and existence of the multiplicative inverse. Using the fact that $(\mathbb{R}, +, \cdot)$ is a field, will we show that all of these properties hold for $(\mathbb{R}, \oplus, \otimes)$.

Property 1: Closure
For any $x, y \in \mathbb{R}$, it follows that $x \oplus y = x + y - 1$. Since $x, y, 1 \in \mathbb{R}$, it follows by the closure of $(\mathbb{R}, +, \cdot)$ that $x + y - 1 \in \mathbb{R}$, and thus $x \oplus y \in \mathbb{R}$. Similarly, for any $x, y \in \mathbb{R}$, it follows that $x \otimes y = x + y - xy$. Since $x, y \in \mathbb{R}$, it follows by the closure of $(\mathbb{R}, +, \cdot)$ that $x + y - xy \in \mathbb{R}$, and thus $x \otimes y \in \mathbb{R}$. Since $(\mathbb{R}, \oplus, \otimes)$ is closed under $\oplus$ and $\otimes$, it follows that $(\mathbb{R}, \oplus, \otimes)$ satisfies the closure property.

Property 2: Associativity
For any $x, y, z \in \mathbb{R}$, we must look at the term $x \oplus (y \oplus z$, and show that it equals $(x \oplus y) \oplus z)$. This is done below.

$$\begin{aligned} x \oplus (y \oplus z) &= x \oplus (y + z - 1) \\ &= x + (y + z - 1) - 1 \\ &= (x + y - 1) + z - 1 \quad \text{(associativty and commutativity of } (\mathbb{R}, +, \cdot)) \\ &= (x \oplus y) + z - 1 \\ &= (x \oplus y) \oplus z \end{aligned}$$

Thus we have shown that $\oplus$ satisfies the associative property. For any $x, y, z \in \mathbb{R}$, we will now look at the term $x \otimes (y \otimes z)$, and show that it equals $(x \otimes y) \otimes z$. This is done below.

$$\begin{aligned} x \otimes (y \otimes z) &= x \otimes (y + z - yz) \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x + y + z - yz - xy - xz + xyz \quad \text{(distributivity of } (\mathbb{R}, +, \cdot)) \\ &= (x + y - xy) + z - yz - xz + xyz \quad \text{(associativty and commutativity of } (\mathbb{R}, +, \cdot)) \\ &= (x \otimes y) + z - yz - xz + xyz \\ &= (x \otimes y) + z - xz - yz + xyz \quad \text{(commutativity of } (\mathbb{R}, +, \cdot)) \\ &= (x \otimes y) + z - (x + y - xy)z \quad \text{(distributivity of } (\mathbb{R}, +, \cdot)) \\ &= (x \otimes y) + z - (x \otimes y)z \\ &= (x \otimes y) \otimes z \end{aligned}$$

Thus we have shown that $\otimes$ satisfies the associative property. Therefore, we have shown that $(\mathbb{R}, \oplus, \otimes)$ satisfies the associative property.

Property 3: Commutativity
For any $x, y \in \mathbb{R}$, we must look at the term $x \oplus y$, and show that it equals $y \oplus x$. This is done below.

$$\begin{aligned} x \oplus y &= x + y - 1 \\ &= y + x - 1 \quad \text{(commutativity of } (\mathbb{R}, +, \cdot)) \\ &= y \oplus x \end{aligned}$$

Thus we have shown that $\oplus$ satisfies the commutative property. For any $x, y \in \mathbb{R}$, we will now look at the term $x \otimes y$, and show that it equals $y \otimes x$. This is done below.

$$\begin{aligned} x \otimes y &= x + y - xy \\ &= y + x - yx \quad \text{(commutativity of } (\mathbb{R}, +, \cdot)) \\ &= y \otimes x \end{aligned}$$

Thus we have shown that $\otimes$ satisfies the commutative property. Therefore, we have shown that $(\mathbb{R}, \oplus, \otimes)$ satisfies the commutative property.

Property 4: Distributivity
For any $x, y \in \mathbb{R}$, we must look at the term $x \otimes (y \oplus z)$, and show that it equals $(x \otimes y) \oplus (x \otimes z)$. This is done below.

$$\begin{aligned} x \otimes (y \oplus z) &= x \otimes (y + z - 1) \\ &= x + (y + z - 1) - x(y + z - 1) \\ &= x + y + z - 1 - xy - xz + x \quad \text{(distributivity of } (\mathbb{R}, +, \cdot)) \\ &= x + y - xy + x + z - xz - 1 \quad \text{(commutativity of } (\mathbb{R}, +, \cdot)) \\ &= (x + y - xy) + (x + z - xz) - 1 \quad \text{(associativty of } (\mathbb{R}, +, \cdot)) \\ &= (x \otimes y) + (x \otimes z) - 1 \\ &= (x \otimes y) \oplus (x \otimes z) \end{aligned}$$

Therefore, we have shown that $(\mathbb{R}, \oplus, \otimes)$ satisfies the distributive property.

Property 5: Additive identity
To show the existence of an additive identity, we must show that there exists an element in $\mathbb{R}$ written a such that for any $x \in \mathbb{R}$, $x \oplus a = x$. To find such an a we will solve $x \oplus a = x$ for a. This is done below.

$$\begin{aligned} x \oplus a = x &\implies x + a - 1 = x \\ &\implies a - 1 = 0 \\ &\implies a = 1 \end{aligned}$$

We will now show that $a = 1$ implies that $x \oplus a = x$. This is done below.

$$\begin{aligned} x \oplus a &= x \oplus 1 \\ &= x + 1 - 1 \\ &= x \end{aligned}$$

Therefore, we have shown that there exists an additive identity in $(\mathbb{R}, \oplus, \otimes)$, which is the real number $a = 1$.

Property 6: Multiplicative identity
To show the existence of a multiplicative identity, we must show that there exists an element in $\mathbb{R}$ written b, that is not $a = 1$ (the additive identity), such that for any $x \in \mathbb{R}$, $x \otimes b = x$. To find such a b we will solve $x \otimes b = x$ for b. This is done below.

$$\begin{aligned} x \otimes b = x &\implies x + b - xb = x \\ &\implies b - xb = 0 \\ &\implies b(1 - x) = 0 \quad \text{(distributivity of } (\mathbb{R}, +, \cdot)) \\ &\implies b = 0 \quad (\text{since } x \neq 1 \implies (1 - x) \neq 0) \end{aligned}$$

We will now show that $b = 0$ implies that $x \otimes b = x$. This is done below.

$$\begin{aligned} x \otimes b &= x \otimes 0 \\ &= x + 0 - x \cdot 0 \\ &= x + 0 - 0 \\ &= x \end{aligned}$$

Therefore, we have shown that there exists a multiplicative identity in $(\mathbb{R}, \oplus, \otimes)$ that is not the additive identity, which is the real number $b = 0$.

Property 7: Additive inverse
To show the existence of an additive inverse, we must show that for any x in $\mathbb{R}$, there exists an element in $\mathbb{R}$ written c such that $x \oplus c = 1$. In other words, $x \oplus c$ equals the additive identity. To find such a c we will solve $x \oplus c = 1$ for c. This is done below.

$$\begin{aligned} x \oplus c = 1 &\implies x + c - 1 = 1 \\ &\implies x + c = 2 \\ &\implies c = 2 - x \end{aligned}$$

We will now show that $c = 2 - x$ implies that $x \oplus c = x$. This is done below.

$$\begin{aligned} x \oplus c &= x \oplus 2 - x \\ &= x + 2 - x - 1 \\ &= 2 - 1 \\ &= 1 \end{aligned}$$

Therefore, we have proven the existence of the additive inverse in $(\mathbb{R}, \oplus, \otimes)$, that is, for any real number x, there exists a real number $c = 2 - x$ such that $x \oplus c = 1$.

Property 8: Multiplicative inverse
To show the existence of a multiplicative inverse, we must show that for any x in $\mathbb{R}$ expect for the additive identity $a = 1$, there exists an element of $\mathbb{R}$ written d such that $x \otimes d = 0$. In other words, $x \otimes d$ equals the multiplicative identity. To find such a d we will solve $x \otimes d = 0$ for d This is done below.

$$\begin{aligned} x \otimes d = 0 &\implies x + d - xd = 0 \\ &\implies d - xd = -x \\ &\implies d(1 - x) = -x \quad \text{(distributivity of } (\mathbb{R}, +, \cdot)) \\ &\implies d = -x(1 - x)^{-1} \quad (\text{since } x \neq 1 \implies (1 - x) \neq 0) \end{aligned}$$

We will now show that $d = -x(1 - x)^{-1}$ implies that $x \otimes d = 0$. This is done below.

$$\begin{aligned} x \otimes d &= x \otimes -x(1 - x)^{-1} \\ &= x - x(1 - x)^{-1} + x^2(1 - x)^{-1} \\ &= x(1 - (1 - x)^{-1} + x(1 - x)^{-1}) \quad \text{(distributivity of } (\mathbb{R}, +, \cdot)) \\ &= x(1 - (1 - x)^{-1}(1 - x)) \quad \text{(distributivity of } (\mathbb{R}, +, \cdot)) \\ &= x(1 - 1) \quad (\text{since } aa^{-1} = 1 \text{ in } (\mathbb{R}, +, \cdot)) \\ &= x \cdot 0 \\ &= 0 \end{aligned}$$

Therefore, we have proven the existence of the multiplicative inverse in $(\mathbb{R}, \oplus, \otimes)$, that is, for any real number x that is not the additive identity, there exists a real number $d = -x(1 - x)^{-1}$ such that $x \otimes d = x$.

Since all eight properties are met, it follows that $(\mathbb{R}, \oplus, \otimes)$ is a commutative field. $\square$

Exercise 3. Assume that $(F, +, \cdot)$ is a commutative field totally ordered.

1. Prove that if $a < b < c$, then $|b| < max(|a|, |c|)$.

Proof: Let $a, b, c \in F$, in order to prove that $|b| < max(|a|, |c|)$, we will focus on two cases. These two cases are: $b < 0$, and $b \geq 0$.

Case 1: b < 0
If $b < 0$, then since $a < b$, it follows that $a < 0$. Furthermore, since $a < 0$ and $b < 0$ by the definition of the absolute value, it follows that $|a| = -a$ and $|b| = -b$. Furthermore, given that $(F, +, \cdot)$ is a commutative field totally ordered, using theorem 1 on slide 5 of the lecture 2 notes, it follows that $-b < -a$. Since $-b < -a$, $|a| = -a$, and $|b| = -b$, this implies that $|b| < |a|$. Therefore, $|b| < |a| \leq max(|a|, |c|)$, which implies that $|b| < max(|a|, |c|)$.

Case 2: b ≥ 0
If $b > 0$, then since $b < c$, it follows that $c > 0$. Furthermore, since $c > 0$ and $b > 0$ by the definition of the absolute value, it follows that $|c| = c$ and $|b| = b$. Since $b < c$, $|c| = c$, and $|b| = b$, this implies that $|b| < |c|$. Therefore, $|b| < |c| \leq max(|a|, |c|)$, which implies $|b| < max(|a|, |c|)$.

Therefore, no matter what the value of b is, we have shown that if $a < b < c$, then $|b| < max(|a|, |c|)$. □

2. Let ϵ be a positive element of F. Prove that $|x| < \epsilon$ if and only if $-\epsilon < x < +\epsilon$.

Proof: Let $\epsilon \in F$ such that $\epsilon > 0$. Furthermore, let $x \in F$. In order to prove that $|x| < \epsilon$ if and only if $-\epsilon < x < +\epsilon$, we must prove both implications. That is, we must first prove that if $|x| < \epsilon$, then $-\epsilon < x < +\epsilon$. Then we must prove that if $-\epsilon < x < +\epsilon$, then $|x| < \epsilon$.

Implication 1:
If we know that $|x| < \epsilon$, then in order to prove that $-\epsilon < x < +\epsilon$, we will focus on two cases. These two cases are: $x < 0$ and $x \geq 0$.

Case 1: x < 0
If $x < 0$, by the definition of the absolute value, it follows that $|x| = -x$. Since we already know that $|x| < \epsilon$ and $|x| = -x$, it follows that $-x < \epsilon$. Furthermore, since $-x < \epsilon$ and $(F, +, \cdot)$ is a commutative field totally ordered, using theorem 1 on slide 5 of the lecture 2 notes, it follows that $-\epsilon < x$. Since we started with the assumption that $x < 0$, and we know that $\epsilon > 0$, it follows that $x < \epsilon$. Putting these two parts together, we have shown that if $|x| < \epsilon$ and $x < 0$, then $-\epsilon < x < +\epsilon$.

Case 2: x ≥ 0
If $x \geq 0$, by the definition of the absolute value, it follows that $|x| = x$. Since we already know that $|x| < \epsilon$ and $|x| = x$, it follows that $x < \epsilon$. Furthermore, since $0 < \epsilon$ and $(F, +, \cdot)$ is a commutative field totally ordered, using theorem 1 on slide 5 of the lecture 2 notes, it follows that $-\epsilon < 0$. Since we started with the assumption that $x \geq 0$, and we know that $-\epsilon < 0$, it follows that $x > -\epsilon$. Putting these two parts together, we have shown that if $|x| < \epsilon$ and $x < 0$, then $-\epsilon < x < +\epsilon$.

Therefore, no matter what the value of x is, we have shown that if $|x| < \epsilon$, then $-\epsilon < x < +\epsilon$.

Implication 2:
If we know that $-\epsilon < x < +\epsilon$, then in order to prove that $|x| < \epsilon$, we will focus on two cases. These two cases are: $x < 0$ and $x \geq 0$.

Case 1: x < 0
If $x < 0$, by the definition of the absolute value, it follows that $|x| = -x$. Furthermore, since $-\epsilon < x$ and $(F, +, \cdot)$ is a commutative field totally ordered, using theorem 1 on slide 5 of the lecture 2 notes, it follows that $-x < \epsilon$. Since $|x| = -x$ and $-x < \epsilon$, it follows that $|x| < \epsilon$. Hence we have shown that, if $x < 0$ and $-\epsilon < x < +\epsilon$, then $|x| < \epsilon$.

Case 2: $\mathbf{x \geq 0}$
If $x \geq 0$, by the definition of the absolute value, it follows that $|x| = x$. Since we already know that $x < \epsilon$ and $|x| = x$, it follows that $|x| < \epsilon$. Hence we have shown that if $x \geq 0$ and $-\epsilon < x < +\epsilon$, then $|x| < \epsilon$.

Therefore, no matter what the value of x is, we have shown that if $-\epsilon < x < +\epsilon$, then $|x| < \epsilon$.

Since we have proven both implications, we have shown that if we let ϵ be a positive element of F, then $|x| < \epsilon$ if and only if $-\epsilon < x < +\epsilon$. $\square$

Exercise 4. In this exercise we work with real numbers. We can use the fact that $\mathbb{R}$ is a commutative field totally ordered, that satisfies the continuity axiom. You may use every property listed in the notes about commutative fields, inequalities, and the continuity axiom. The goal of this exercise is to prove that for any positive real number m, the square root of m exists. It means that until the end of the exercise, we don't even know the square root exists. The idea of the proof is to create a set L such that its least upper bound is exactly the square root of m. The first step is to justify the existence of the least upper bound c of L. The second step is to prove that the least upper bound c of L satisfies $c^2 = m$, i.e. c is the square root of m. Let's start the proof: Given a positive real number m,

1. Let x and z be 2 positive real numbers, prove that if $x^2 < z^2$ then $x < z$.

Since I came up with two proofs for this problem, I will present them both.

Proof 1: (Proof by contrapositive) To prove the above theorem, we will prove the contrapositive, which is "If $x \geq z$, then $x^2 \geq z^2$." Let x and z be two positive real numbers. That is, $x, z \in \mathbb{R}$, $x > 0$, and $z > 0$. If $x \geq z$, then since the real numbers are totally ordered, using theorem 1 on slide 5 of the lecture 2 notes with $a = z$, $b = x$, and $c = x$, it follows that $x \cdot x = x^2 \geq xz$. Furthermore, if $x \geq z$, then since the real numbers are totally ordered, using theorem 1 on slide 5 of the lecture 2 notes with $a = z$, $b = x$, and $c = z$, it follows that $xz \geq z \cdot z = z^2$. Since $x^2 \geq xz \geq z^2$, and the real numbers are totally ordered, using definition 3 on page 3 of the lecture 2 notes, it follows that $x^2 \geq z^2$. Hence we have shown that, if $x \geq z$, then $x^2 \geq z^2$. Therefore, we have proven that if $x^2 < z^2$, then $x < z$. $\square$

Proof 2: Let x and z be two positive real numbers. That is, $x, z \in \mathbb{R}$, $x > 0$, and $z > 0$. If $x^2 < z^2$, then adding the additive inverse of x^2 on both sides we obtain $0 < z^2 - x^2$. Using the distributive property twice, we obtain $0 < (z - x)(z + x)$. Since $x > 0$ and $z > 0$ implies that $x + z \neq 0$, then the multiplicative inverse exists, and we can multiply $z + x$ on both sides of the inequality. Since $0 < (z + x)$, and the real numbers are totally ordered, using definition 5 on page 3 of the lecture 2 notes, when we multiply by $z + x$ on both sides of the inequality, it follows that $0 < z - x$. Adding the additive inverse of $-x$ on both sides we obtain $x < z$. Therefore, we have proven that if $x^2 < z^2$, then $x < z$. $\square$

2. Let $L = \{x$ such that $0 < x$ and $x^2 < m\}$. Prove that L is not empty and L is bounded above.

We will split this problem into two proofs; proving that L is not empty, and proving that L is bounded above.

Proof 1: If we let m be a positive real number and the set L be defined as $L = \{x$ such that $0 < x$ and $x^2 < m\}$, then to prove that L is not empty, we will focus on two cases. These two cases are $m > 1$ and $m \leq 1$.

Case 1: m > 1
If $m > 1$, then since $1 > 0$ and $1^2 = 1 \cdot 1 = 1 < m$ it follows that $x = 1 \in L$. Thus we have shown that, when $m > 1$, L is not empty.

Case 2: m ≤ 1
If $0 < m \leq 1$, then by the Archimedian law of real numbers, there exists a positive integer n such that $1 < mn$. Since $n \in \mathbb{N}$, it follows that $n > 0$, therefore the multiplicative inverse exists and we can see that $\frac{1}{n} < m$. Furthermore, since $0 < n \leq n^2$ and the real numbers are totally ordered, using theorem 9 on page 5 of the lecture 2 notes, we know that $\frac{1}{n^2} \leq \frac{1}{n}$ and thus $\frac{1}{n^2} \leq \frac{1}{n} < m$. If we let $x = \frac{1}{n}$, since $\frac{1}{n} > 0$ and $\frac{1}{n^2} < m$, it follows that $x = \frac{1}{n} \in L$. Thus we have shown that, when $m \leq 1$, L is not empty.

Therefore, whatever the value of m is, we have shown that the set L is not empty. $\square$

Proof 2: If we let m be a positive real number and the set L be defined as $L = \{x$ such that $0 < x$ and $x^2 < m\}$, then to prove that L is bounded above we must notice that, since $0 < 1$ and the real numbers are totally ordered, using theorem 6 on page 5 of the lecture 2 notes, we know that $m < m + 1$. Furthermore, using theorem 7 on page 5 of the lecture 2 notes, we know that $m < (m+1)^2$. Now, $\forall x \in L$, we know that $x^2 < m$, however, since $m < (m+1)^2$, we also know that $x^2 < (m+1)^2$. Using the results from part 1 of this exercise we know that $x < m+1$. That means we have just shown that, $\forall x \in L$, it follows that $x < m+1$. Therefore,

by the definition of an upper bound, $m+1$ is an upper bound for L. Therefore, we have shown that L is bounded above. $\square$

3. Let c be the least upper bound of L.

(a) Justify the existence of c.

Since the set L is not empty no matter what m is chosen, and the fact that L is bounded above by $m+1$ no matter what m is chosen, by the continuity axiom, $\exists c \in \mathbb{R}$ such that $\forall x \in L$, $x \leq c$. In this case c is called the least upper bound of L or the supremum of L.

(b) Prove that $c^2 = m$

Proof: (Proof by contradiction) Assume for the sake of contradiction that $c^2 \neq m$. Then in order to find a contradiction we will work with two cases. These two cases are $c^2 < m$ and $c^2 > m$.

Case 1: $\mathbf{c^2 < m}$
Since $c^2 < m$ and $c > 0$, by the definition of L, it follows that $c \in L$. Since c is supposed to be an upper bound, and in our current case is an element in L, that means that there can be no element in L greater than c. In order to violate the fact that c is an upper bound, we are in search of an element in L larger than c. Note that one such element is $c + \frac{1}{n}$, where $n \in \mathbb{N}$. To show that this element is in L we will look at the term $(c+\frac{1}{n})^2$. We can see from using the distributive property twice that $(c+\frac{1}{n})^2 = c^2 + \frac{2c}{n} + \frac{1}{n^2}$. As shown in part 2 of this exercise, $\frac{1}{n^2} \leq \frac{1}{n}$, thus we can see that $(c+\frac{1}{n})^2 = c^2 + \frac{2c}{n} + \frac{1}{n^2} \leq c^2 + \frac{2c}{n} + \frac{1}{n} = c^2 + \frac{2c+1}{n}$. Since $c^2 < m$ implies that $0 < m - c^2$, we are in essence searching for an n such that adding $\frac{2c+1}{n}$ to c^2 keeps the total less than m. In order to add $\frac{2c+1}{n}$ to c^2 and have it be less than m, we must find the n such that $2c+1 < (m-c^2)n \implies \frac{2c+1}{n} < m - c^2$. Since $2c+1 > 0$ and $m - c^2 > 0$, by the Archimedian law of real numbers, this n exists and we will call it n_*. Therefore we can see that $(c+\frac{1}{n_*})^2 \leq c^2 + \frac{2c+1}{n_*} < c^2 + (m-c^2) = m$. Since $(c+\frac{1}{n_*})^2 < m$, it follows that $c + \frac{1}{n_*} \in L$, therefore we have found an element greater than c that is in L. This contradicts the fact that c is an upper bound of L. Thus our assumption that $c^2 < m$ was wrong.

Case 2: $\mathbf{c^2 > m}$
Since $c^2 > m$, in order to violate the fact that c is the least upper bound, we are in search of an upper bound smaller than c. Note that one such element that is smaller than c is $c - \frac{1}{n}$, where $n \in \mathbb{N}$. To show that this element is smaller than c while still being an upper bound to L we will look at the term $(c-\frac{1}{n})^2$. We can see from using the distributive property twice that $(c-\frac{1}{n})^2 = c^2 - \frac{2c}{n} + \frac{1}{n^2}$. Since $n > 0$ it follows that $\frac{1}{n^2} > 0$, thus we can see that $(c-\frac{1}{n})^2 = c^2 - \frac{2c}{n} + \frac{1}{n^2} > c^2 - \frac{2c}{n}$. Since $c^2 > m$ implies that $c^2 - m > 0$, we are in essence searching for an n such that subtracting $\frac{2c}{n}$ from c^2 keeps the total greater than m. In order to subtract $\frac{2c}{n}$ from c^2 and have it be greater than m, we must find the n such that $2c < (c^2-m)n \implies \frac{2c}{n} < c^2 - m$. Since $2c > 0$ and $c^2 - m > 0$, by the Archimedian law of real numbers, this n exists and we will call it n_*. Therefore we can see that $(c-\frac{1}{n_*})^2 > c^2 - \frac{2c}{n_*} > c^2 - (c^2 - m) = m$. Since $(c-\frac{1}{n_*})^2 > m$, it follows that $\forall x \in L$, $x^2 < m < (c-\frac{1}{n_*})^2$. Using the result proven in part 1 of the exercise, we see that $x < c - \frac{1}{n_*}$ for all $x \in L$. Therefore we have found an element less than c that is also an upper bound of the set L. This contradicts the fact that c is the least upper bound of L. Thus our assumption that $c^2 > m$ was wrong.

Since $c^2 < m$ and $c^2 > m$ are wrong, it follows that our assumption that $c^2 = m$ was wrong. Therefore $c^2 = m$ and hence we have shown that c is the square root of m. $\square$.

Appendix.
In this section, theorems that we didn't prove in class will be proven so that they can be used in the exercises.

1. If $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

Proof: (Proof by contrapostive) To prove the above theorem, we will prove the contrapositive, which is "If $ab = 0$, then $a = 0$ or $b = 0$." Without loss of generality, say $b \neq 0$. Then, if $ab = 0$ and $b \neq 0$, by the definition of a multiplicative inverse, b^{-1} exists. Therefore we can see that $0 = 0 \cdot b^{-1} = (ab) \cdot b^{-1} = a \cdot (bb^{-1}) = a \cdot 1 = a$. Hence $a = 0$. This means that we have shown that, if $ab = 0$, then $a = 0$ or $b = 0$. Therefore, since we have proven the contrapositive as true, we have shown that, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$. $\square$

2. If $ab \neq 0$, then $a \neq 0$ and $b \neq 0$.

Proof: (Proof by contrapostive) To prove the above theorem, we will prove the contrapositive, which is "If $a = 0$ or $b = 0$, then $ab = 0$." We will prove this by cases. The three possible cases are: $a = 0$ and $b = 0$, $a = 0$ and $b \neq 0$, and, $a \neq 0$ and $b \neq 0$. If $a = 0$ and $b = 0$, then $a \cdot b = 0 \cdot 0 = 0$. If $a = 0$ and $b \neq 0$, then $a \cdot b = 0 \cdot b = 0$. Lastly, if $a \neq 0$ and $b = 0$, the $a \cdot b = a \cdot 0 = 0$. This means that we have shown that, if $a = 0$ or $b = 0$, then $ab = 0$. Therefore, since we have proven the contrapositive as true, we have shown that, if $ab \neq 0$, then $a \neq 0$ and $b \neq 0$. $\square$