# Homework 3

Jim Zieleman

September 14, 2020

Extra Credit 1. *Show that if $a \in Z$, then $a$ is either even, or odd, but not both.*
Proof:
Let $a \in Z$ such that $a$ is even and odd.
Since $a$ is even then 2 divides $a$ by definition 2.
Let $c \in Z$ so $2 \cdot c = a$ by definition 1.
Since $a$ is odd then 2 divides $a - 1$ by definition 2.
Let $d \in Z$ so $2 \cdot d = a - 1$ by definition 1.
So $2 \cdot d + 1 = a$.
Then $2 \cdot d + 1 = 2 \cdot c$.
Then $1 = 2 \cdot c - 2 \cdot d = 2(c - d)$.
Then $1 = 2(c - d)$.
We have reached a contradiction since $c - d$ will be an integer, however there exists no integer that is the product of 2 dividing 1. So $a$ must either be even, or odd, but not both.

1. Let $a \in Z$.

   (a) Prove that if $a$ is even, then 4 divides $a^2$.
   Proof:
   If $a$ is even.
   Then 2 divides $a$.
   Then $2 \cdot c = a$.
   Then $a(2 \cdot c) = a \cdot a$.
   Then $(2 \cdot c)(2 \cdot c) = a^2$.
   Then $4c^2 = a^2$.
   Then $4d = a^2$ where $c^2 = d$ and $d \in Z$.
   So by definition 1, 4 divides $a^2$.
   Thus if $a$ is even, 4 divides $a^2$.
   Corallary: If 4 divides some $a \in Z$, then 2 divides $a$, thus if a is even, 2 divides $a^2$ and is even.

   (b) Prove that if $a$ is odd, then $a^2$ is odd.
   Proof:
   If $a$ is odd.
   Then 2 divides $a - 1$.
   Then $2 \cdot c = a - 1$.

Then $2 \cdot c + 1 = a$.
Then $a(2 \cdot c + 1) = a \cdot a$.
Then $(2 \cdot c + 1)(2 \cdot c + 1) = a^2$.
Then $4c^2 + 4c + 1 = a^2$.
Then $2(2c^2 + 2c) + 1 = a^2$.
Then $2 \cdot d + 1 = a^2$ where $d \in Z$ and $2c^2 + 2c = d$.
Then $2 \cdot d = a^2 - 1$.
So by definition 1, 2 divides $a^2 - 1$.
Thus if $a$ is odd, $a^2$ is odd.

(c) Explain why parts (a) and (b) prove that an integer $a$ is even if and only if $a^2$ is even.
Explaination:
Both part a and b show that if a is even then $a^2$ is even, and if a is odd then $a^2$ is odd. Since this was proved directly we can see the other side of the if statement holds up too hence proving the iff statement.

2. Suppose that there exists integers $a$ and $b$ such that $(a/b)^2 = 2$.

(a) Explain why this implies there exists integers $a', b'$ such that $(a'/b')^2 = 2$ and $a', b'$ have no common divisors (i.e., there are no integers $d > 1$ such that $d$ divides both $a$ and $b$).
Proof:
Let $d \in Z > 1$ where $d$ represents all common divisors of both $a$ and $b$.
$a = a' \cdot d$ and $b = b' \cdot d$.
Then $a/b = (a' \cdot d)/(b' \cdot d) = a'/b'$.
So in the case of $(a/b)^2 = (a'/b')^2 = 2$ and $(a'/b')^2$ has no common divisors other than 1.

(b) Explain why at most one of $a'$ and $b'$ is even. If $a'$ is even and $b'$ is even then they both have 2 as a common divisor. Thus only 1 can be even.

(c) Explain why $a'$ must be even.
$(a'/b')^2 = 2$.
$(a'/b')(a'/b') = 2$.
$(a')(a'/b') = 2b'$.
$(a')(a') = 2b'b'$.
$a'^2 = 2b'^2$.
2 divides $a'^2$ so it must be even. So $a'$ is even.

(d) Explain why part (c) implies that $b'$ must be even as well.
If $a'^2$ is even by (1a), 4 divides $a'^2$.
$4 \cdot c = a'^2$.
$4 \cdot c = 2b'^2$.
$2 \cdot c = b'^2$.
So 2 divides $b'^2$ so it must be even. So then $b'$ is even.

(e) Explain the contradiction between parts (b), (c), and (d).
We have a contradiction because in part (c) and (d) both $a'$ and $b'$ are even and in part (b) we know only one can be even.

(f) Explain why this implies there is no rational number $r$ satisfying $r^2 = 2$ (that is, $\sqrt{2}$ is not rational).
By representing $(a/b)^2 = 2$ as $(a'/b')^2 = 2$ where $a'/b'$ is an irreducible rational number we get the contradiction shown in part (e). Thus we cannot make the assumption that $a/b$ is a rational number, implying there is no rational number $r$ satisfying $r^2 = 2$.

3. Prove that $A$ has a least upper bound in $R$.
Let $A := \{x \in R | x^2 < 2\}$.
Let $x = 1$ then $1^2 = 1 < 2$ so $1 \in A$.
So $A$ is non empty.
Let $x > 2$ then $x^2 > 2^2$ so $x^2 > 4 > 2$.
So $A$ has a least upper bound in $R$.
We will denote it as $\alpha$.

4. Define $\alpha$ as above. In this problem we will show that $2 \leq \alpha^2$ by contradiction.

Suppose that $\alpha^2 < 2$, and define:

$$h = \frac{(2 - \alpha^2)}{2(2\alpha + 1)}$$

(a) Explain why $0 < \alpha$ and use this to show $0 < h < 1$.
The lub(A) is $\alpha$ and $x \in A$ such that $x > 0$ so $0 < x < \alpha$.
Since $\alpha^2 < 2$ then $0 < 2 - \alpha^2$ so $h$ is positive.
$h = \frac{1}{2\alpha+1}(1 - \frac{\alpha^2}{2})$.
Since $\frac{\alpha^2}{2} < 1$ then $1 - \frac{\alpha^2}{2} < 1$ and $\frac{1}{2\alpha+1} < 1$.
So $h < 1$.
Thus $0 < h < 1$.

(b) Show that $(\alpha + h)^2 < \alpha^2 + 2\alpha h + h = \alpha^2 + h(2\alpha + 1)$.
We know $0 < \alpha^2 < 2$ and $0 < h < 1$.
$(\alpha + h)^2 = \alpha^2 + 2\alpha h + h^2$.
Let $k \in Z$ such that $h = 1/k$ and $h^2 = 1/k^2$.
$k^2 > k$ so $1/k^2 < 1/k$.
So $h^2 < h$.
Then $(\alpha + h)^2 < \alpha^2 + 2\alpha h + h = \alpha^2 + h(2\alpha + 1)$.

(c) Show that the previous part implies that $(\alpha + h)^2 < \frac{(2+\alpha^2)}{2} < 2$.
$h = \frac{(2-\alpha^2)}{2(2\alpha+1)}$
$h(2\alpha + 1) = \frac{(2-\alpha^2)}{2}$
$\alpha^2 + h(2\alpha + 1) = \frac{(2+\alpha^2)}{2}$
So $(\alpha + h)^2 < \frac{(2+\alpha^2)}{2}$.

Since $\alpha^2 < 2$ then $\frac{(\alpha^2)}{2} < 1$ so $1 + \frac{(\alpha^2)}{2} < 2$.
$1 + \frac{(\alpha^2)}{2} = \frac{2+\alpha^2}{2} < 2$.
Thus $(\alpha + h)^2 < \frac{(2+\alpha^2)}{2} < 2$.

(d) Explain why $\alpha + h \in A$ and $\alpha < \alpha + h$.
We showed $(\alpha + h)^2 < 2$ thus every element squared that is less than 2 is in the set A. Thus $\alpha + h \in A$.
We showed since $0 < \alpha$ and $0 < h$ then $\alpha < \alpha + h$.

(e) Explain why $(d)$ is a contradiction.
We started by assuming $\alpha$ was lub(A) which meant there was no $a \in A$ such that $\alpha < a$. Then by assuming $\alpha^2 < 2$ we found an element $a \in A$ that showed $\alpha < a$ this is a contradiction so $\alpha^2 \geq 2$.

5. Now we will finish the proof that $\alpha^2 = 2$.
Working by contradiction again, suppose that $\alpha^2 \neq 2$. By the previous problem, we must have $2 < \alpha^2$. Define

$$k = \frac{\alpha^2 - 2}{4\alpha}$$

.

(a) Show that $\alpha - k < \alpha$.
$\alpha^2 > 2$ so $\alpha^2 - 2 > 0$.
$\alpha > 0$ so $4\alpha > 0$.
So $k > 0$.
Then $\alpha - k < \alpha$.

(b) Show that $\alpha^2 - 2\alpha k < (\alpha - k)^2$.
$(\alpha - k)^2 = \alpha^2 - 2\alpha k + k^2$.
Since $k > 0$ then $k^2 > 0$.
So $\alpha^2 - 2\alpha k + k^2 > \alpha^2 - 2\alpha k + k^2 - k^2$.
So $\alpha^2 - 2\alpha k + k^2 = (\alpha - k)^2 > \alpha^2 - 2\alpha k$.
Thus $\alpha^2 - 2\alpha k < (\alpha - k)^2$.

(c) Show that the previous part implies that $2 < \frac{\alpha^2+2}{2} < (\alpha - k)^2$.
$\alpha^2 - 2\alpha k < (\alpha - k)^2$.
$\alpha^2 - 2\alpha(\frac{\alpha^2-2}{4\alpha}) < (\alpha - k)^2$.
$\alpha^2 - \frac{\alpha^2-2}{2} < (\alpha - k)^2$.
$\frac{\alpha^2+2}{2} < (\alpha - k)^2$.
$\alpha^2 > 2$ so $\frac{\alpha^2}{2} > 1$ so $\frac{\alpha^2}{2} + 1 > 2$.
So $2 < \frac{\alpha^2+2}{2} < (\alpha + k)^2$.

(d) By part (c), we have $2 < (\alpha - k)^2$. Use this to show that $\alpha - k$ is an upper bound for $A$.
$2 < (\alpha - k)^2$.
Then $\alpha - k \in A$ and it is an upper bound.
Thus $\alpha < \alpha - k$.

(e) Explain why parts (a) and (d) give a contradiction to the definition of $\alpha$.
Part (a) says $\alpha - k < \alpha$.
Part (d) contradicts this by saying $\alpha < \alpha - k$.
So $\alpha \not< 2$ and $\alpha \not> 2$ so $\alpha = 2$.
Thus lub(A) is $\alpha = 2$.

6. In this problem, we will prove the following theorem.

Theorem 1 (Archimedean Property).Suppose that $x, y \in R$ and that $x > 0$. Then there exists an integer $n > 0$ such that $y < nx$.

We will prove the statement by contradiction. Let $A = \{nx | n \in N\}$, and suppose that $A$ is bounded above by $y$.

(a) Let $\alpha = lub(A)$. Show that, for any $r < \alpha$, there exists some $n \in N$ such that $r < nx$. (If $r < \alpha$, can $r$ be an upper bound for $A$? What does that mean?)
$\alpha = lub(A)$
$r \in A$ and $r < \alpha$
Let $r = kx$ where $k \in N$
Let $n \in N$ such that $n = k + 1$
Then $r < (k + 1)x$
Then $r < nx$
So if $r < \alpha$, then $r$ cannot be an upper bound for $A$ since $\alpha$ is the $lub(A)$.

(b) Explain why there exists some $m \in N$ such that $\alpha - x < mx$.
We know if $\alpha$ is the $lub(A)$ then $\alpha - x \in A$.
We know for $r \in A$ there exists $m \in N$ such that $r < mx$
So $\alpha - x < mx$

(c) Explain why the previous part implies $\alpha < (m + 1)x$.
$\alpha - x < mx$
$\alpha < mx + x$
$\alpha < (m + 1)x$

(d) Explain why this gives a contradiction and why this contradiction proves the Archimedean Property.
$(m + 1)x = nx$
$nx \in A$ so $nx > \alpha$
Hence we have a contradiction as no element in $A$ can be larger than $\alpha$ the lub(A). So there exists no lub(A). Any multiple n of some x will always have a larger number. Hence in R there will always exist a multiple n of some x that will be larger than some multiple m of x.