PMATH 333, Solutions to the Exercises for Chapter 1

1: Let R be a ring and let F be a field.

(a) Using only the rules R1-R9 which define a field, prove that for all $a \in F$ if $a \cdot a = a$ then ($a = 0$ or $a = 1$).

Solution: Let $a \in F$. Suppose that $a \cdot a = a$. Suppose that $a \neq 0$. Using R9, since $a \neq 0$ we can choose $b \in F$ so that $a \cdot b = b \cdot a = 1$. Then we have

$$\begin{aligned} a &= 1 \cdot a \text{ , by R6} \\ &= (b \cdot a) \cdot a \text{ , since } b \cdot a = 1 \\ &= b \cdot (a \cdot a) \text{ , by R5} \\ &= b \cdot a \text{ , since } a \cdot a = a \\ &= 1 \text{ , since } b \cdot a = 1. \end{aligned}$$

This proves that if $a \neq 0$ then $a = 1$ or, equivalently, that either $a = 0$ or $a = 1$.

(b) Using only the rules R1-R9, prove that for all $a \in F$ if $a \cdot a = 1$ then ($a = 1$ or $a + 1 = 0$).

Solution: Let $a \in F$. Suppose that $a \cdot a = 1$. Suppose that $a + 1 \neq 0$. Using $R9$, choose $b \in F$ so that $(a + 1) \cdot b = b \cdot (a + 1) = 1$. Then

$$\begin{aligned} a &= a \cdot 1 \text{ , by R6} \\ &= a \cdot ((a + 1) \cdot b) \text{ , since } (a + 1) \cdot b = 1 \\ &= (a \cdot (a + 1)) \cdot b \text{ , by R5} \\ &= (a \cdot a + a \cdot 1) \cdot b \text{ , by R7} \\ &= (1 + a \cdot 1) \cdot b \text{ , since } a \cdot a = a \\ &= (1 + a) \cdot b \text{ , by R6} \\ &= (a + 1) \cdot b \text{ , by R2} \\ &= 1 \text{ , since } (a + 1) \cdot b = 1. \end{aligned}$$

This proves that if $a + 1 \neq 0$ then $a = 1$ or, equivalently, that either $a = 1$ or $a + 1 = 0$.

(c) Using only the rules R1-R7 which define a ring, together with the rule R0 which states that for all $a \in R$ we have ($a \cdot 0 = 0$ and $0 \cdot a = 0$), prove that for all $a, b, c, d \in R$, if $a + c = 0$ and $b + d = 0$ then $ab = cd$.

Solution: Let $a, b, c, d \in R$. Suppose that $a + c = 0$ and $b + d = 0$. Then

$$\begin{aligned} ab &= ab + 0 \text{ , by R3} \\ &= ab + c0 \text{ , by R0} \\ &= ab + c(b + d) \text{ , since } b + d = 0 \\ &= ab + (cb + cd) \text{ , by R7} \\ &= (ab + cb) + cd \text{ , by R1} \\ &= (a + c)b + cd \text{ , by R7} \\ &= 0b + cd \text{ , since } a + c = 0 \\ &= 0 + cd \text{ , by R0} \\ &= cd + 0 \text{ , by R2} \\ &= cd \text{ , by R3.} \end{aligned}$$

2: Let S be an ordered set and let F be an ordered field.

(a) Using only the rules O1-O3, and the rule O0 which defines the strict order $<$ by stating that for all $a, b \in S$ we have $a < b \iff (a \leq b \text{ and } a \neq b)$, prove that for all $a, b, c \in S$, if $a \leq b$ and $b < c$ then $a < c$.

Solution: Let $a, b, c \in S$. Suppose that $a \leq b$ and $b < c$. Since $b < c$ we have $b \leq c$ and $b \neq c$ by O0. Since $a \leq b$ and $b \leq c$ we have $a \leq c$ by O3. Suppose, for a contradiction, that $a = c$. Since $a \leq b$ and $a = c$ we have $c \leq b$ (by substitution). Since $b \leq c$ and $c \leq b$ we have $b = c$ by O2. But $b \neq c$, so we have obtained the desired contradiction, and so $a \neq c$. Since $a \leq c$ and $a \neq c$ we have $a < c$ by O0.

(b) Using only the rules R1-R9 and O1-O5, prove that for all $a, b \in F$ if $0 \leq a$ and $a \leq b$ then $a \cdot a \leq b \cdot b$.

Solution: Let $a, b \in F$. Suppose that $0 \leq a$ and $a \leq b$. Since $0 \leq a$ and $a \leq b$ we have $0 \leq b$ by O3. Using R4, choose $c \in F$ so that $a + c = 0$. Since $a \leq b$ we have $a + c \leq b + c$ by O4, and hence $0 \leq b + c$ since $a + c = 0$. Since $0 \leq a$ and $0 \leq b + c$ we have $0 \leq a(b + c)$ by O5. Also, since $0 \leq b + c$ and $0 \leq b$ we have $0 \leq (b + c)b$. Thus

$$\begin{aligned}
0 &\leq a(b+c) \\
0 + aa &\leq a(b+c) + aa \text{ , by O4} \\
aa + 0 &\leq a(b+c) + aa \text{ , by R2} \\
aa &\leq a(b+c) + aa \text{ , by R3} \\
aa &\leq (ab+ac) + aa \text{ , by R7} \\
aa &\leq ab + (ac+aa) \text{ , by R1} \\
aa &\leq ab + a(c+a) \text{ , by R7} \\
aa &\leq ab + a(a+c) \text{ , by R2} \\
aa &\leq ab + a0 \text{ , since } a+c=0 \\
aa &\leq a(b+0) \text{ , by R7} \\
aa &\leq ab \text{ , by R3}
\end{aligned}$$

and

$$\begin{aligned}
0 &\leq (b+c)b \\
0 + ab &\leq (b+c)b + ab \text{ , by O4} \\
ab + 0 &\leq (b+c)b + ab \text{ , by R2} \\
ab &\leq (b+c)b + ab \text{ , by R3} \\
ab &\leq (bb+cb) + ab \text{ , by R7} \\
ab &\leq bb + (cb+ab) \text{ , by R1} \\
ab &\leq bb + (c+a)b \text{ , by R7} \\
ab &\leq bb + (a+c)b \text{ , by R2} \\
ab &\leq bb + 0b \text{ , since } a+c=0 \\
ab &\leq (b+0)b \text{ , by R7} \\
ab &\leq bb \text{ , by R3}
\end{aligned}$$

Since $aa \leq ab$ and $ab \leq bb$ we have $aa \leq bb$ by O3.

(c) Using only rules R1-R9 and O1-O5, together with the rule R0 from Exercise 1(c), prove that $0 \leq 1$.

Solution: Choose $u \in R$ so that $1 + u = 0$ (we can do this by R4). Then

$$\begin{aligned}
u \cdot u &= u \cdot u + 0 \text{ , by R3,} \\
&= u \cdot u + 0 \cdot 1 \text{ , by R6,} \\
&= u \cdot u + (1+u) \cdot 1 \text{ , since } 1+u=0, \\
&= u \cdot u + (1 \cdot 1 + u \cdot 1) \text{ , by R7.} \\
&= (1 \cdot 1 + u \cdot 1) + u \cdot u \text{ , by R2.} \\
&= 1 \cdot 1 + (u \cdot 1 + u \cdot u) \text{ , by R1,} \\
&= 1 \cdot 1 + u \cdot (1+u) \text{ , by R7,} \\
&= 1 \cdot 1 + u \cdot 0 \text{ , since } 1+u=0, \\
&= 1 \cdot 1 + 0 \text{ , by R0,} \\
&= 1 \cdot 1 \text{ , by R3,} \\
&= 1 \text{ , by R6.}
\end{aligned}$$

By O1 we know that either $0 \leq 1$ or $1 \leq 0$. Suppose, for a contradiction, that $1 \leq 0$. Then

$$\begin{aligned}
1 + u &\leq 0 + u \text{ , by O4,} \\
0 &\leq 0 + u \text{ , since } 1+u=0, \\
0 &\leq u + 0 \text{ , by R2,} \\
0 &\leq u \text{ , by R3,} \\
0 &\leq u \cdot u \text{ , by O5,} \\
0 &\leq 1 \text{ , since } u \cdot u = 1 \text{, as shown above.}
\end{aligned}$$

Since $0 \leq 1$ and $1 \leq 0$ we have $0 = 1$ by O2. This gives the desired contradiction because $0 \neq 1$, from the definition of a ring.

3: In this problem, you may use any of the algebraic properties and order properties of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ described in Chapter 1 of the Lecture Notes.

(a) Let $A = \left\{(-1)^n + \frac{1}{n} \,\middle|\, n \in \mathbb{Z}^+\right\}$. Find (with proof) $\sup A$ and $\inf A$.

Solution: We claim that $\sup A = \frac{3}{2}$. Let $x \in A$, say $x = (-1)^n + \frac{1}{n}$ where $1 \le n \in \mathbb{Z}$. If n is even then $(-1)^n = 1$ and $n \ge 2$ so that $\frac{1}{n} \le \frac{1}{2}$, and so we have $x = (-1)^n + \frac{1}{n} = 1 + \frac{1}{n} \le 1 + \frac{1}{2} = \frac{3}{2}$. If n is odd then $(-1)^n = -1$ and $n \ge 1$ so that $\frac{1}{n} \le 1$, and so we have $x = (-1)^n + \frac{1}{n} = -1 + \frac{1}{n} \le -1 + 1 = 0 \le \frac{3}{2}$. In either case, we have $x \le \frac{3}{2}$. Thus $x \le \frac{3}{2}$ for all $x \in A$, and so $\frac{3}{2}$ is an upper bound for A in $\mathbb{R}$. If $c \in \mathbb{R}$ is any upper bound for A then $c \le x$ for all $x \in A$, and in particular $c \le (-1)^2 + \frac{1}{2} = \frac{3}{2}$. Thus $\frac{3}{2} = \sup A$.

We claim that $\inf A = -1$. Let $x \in A$, say $x = (-1)^n + \frac{1}{n}$ with $1 \le n \in \mathbb{Z}$. Since $(-1)^n \ge -1$ and $\frac{1}{n} > 0$ we have $x = (-1)^n + \frac{1}{n} > -1 + 0 = -1$. Since $x > -1$ for all $x \in A$ we see that -1 is a lower bound for A in $\mathbb{R}$. Let $c \in \mathbb{R}$ be any lower bound for A. Suppose, for a contradiction, that $c > -1$. Then $c + 1 > 0$ hence $\frac{1}{c+1} > 0$. Choose an odd integer $n \in \mathbb{Z}$ with $n > \frac{1}{c+1} > 0$ (we are using the Archimedean Property here) and note that $\frac{1}{n} < c + 1$. Let $x = (-1)^n + \frac{1}{n}$. Then $x \in A$ with $x = (-1)^n + \frac{1}{n} = -1 + \frac{1}{n} < -1 + (c+1) = c$, which contradicts the fact that c is a lower bound for A. Thus we must have $c \le -1$. Since -1 is a lower bound for A and since every lower bound c for A satisfies $c \le -1$, it follows that $-1 = \inf A$, as claimed.

(b) Prove that for every $0 \le y \in \mathbb{R}$ there exists a unique $0 \le x \in \mathbb{R}$ such that $x^2 = y$ (this number x is called the *square root* of y and is denoted by $x = \sqrt{y} = y^{1/2}$). In other words, prove that the function $f : [0, \infty) \to [0, \infty)$ given by $f(x) = x^2$ is bijective.

Solution: First we prove uniqueness. Suppose that $x_1 \ge 0$ and $x_2 \ge 0$ and ${x_1}^2 = {x_2}^2 = y$. Since ${x_1}^2 = {x_2}^2$ we have $(x_1 - x_2)(x_1 + x_2) = {x_1}^2 - {x_2}^2 = 0$ and hence either $x_1 - x_2 = 0$ or $x_1 + x_2 = 0$ (since a field has no zero divisors). In the case that $x_1 + x_2 = 0$, since $x_1 \ge 0$ and $x_2 \ge 0$ we must have $x_1 = x_2 = 0$ (indeed if we had $x_2 > 0$ then we would have $x_1 = -x_2 < 0$, so we must have $x_2 = 0$, and hence $x_1 = -x_2 = -0 = 0$). In the case that $x_1 - x_2 = 0$ we have $x_1 = x_2$. In either case, we have $x_1 = x_2$. This proves uniqueness.

Next we prove existence. Let $0 \le y \in \mathbb{R}$. Let $A = \left\{0 \le t \in \mathbb{R} \middle| t^2 \le y\right\}$. Note that $A \ne \emptyset$ since $0 \in A$. We claim that A is bounded above. If $0 \le y \le 1$ then A is bounded above by 1 because $t > 1 \implies t^2 > 1 \implies t^2 > y \implies t \notin A$. If $y \ge 1$ then A is bounded above by y because $t > y \ge 1 \implies t^2 > y^2 > y \implies t \notin A$. In either case, A is bounded above. Since $A \ne \emptyset$ and A is bounded above, we know that A has a supremum in $\mathbb{R}$ by the Completeness Property of $\mathbb{R}$. Let $x = \sup A$. We claim that $x^2 = y$. Suppose, for a contradiction, that $x^2 < y$. Note that for $0 < \epsilon \le 1$ we have $(x + \epsilon)^2 = x^2 + 2x\epsilon + \epsilon^2 \le x^2 + 2x\epsilon + \epsilon = x^2 + (2x+1)\epsilon$ and we have $x^2 + (2x+1)\epsilon \le y \iff \epsilon \le \frac{y - x^2}{2x+1}$. Choose $\epsilon = \min\left\{1, \frac{y-x^2}{2x+1}\right\}$. Then $(x+\epsilon)^2 \le x^2 + (2x+1)\epsilon \le y$ so that $x + \epsilon \in A$, which contradicts the fact that $x = \sup A$. Thus we must have $x^2 \ge y$. Now suppose, for a contradiction, that $x^2 > y$. Note that for $0 < \epsilon \le x$ we have $(x - \epsilon)^2 = x^2 - 2x\epsilon + \epsilon^2 > x^2 - 2x\epsilon$ and we have $x^2 - 2x\epsilon \ge y \iff \epsilon \le \frac{x^2 - y}{2x}$. Choose $\epsilon = \min\left\{x, \frac{x^2-y}{2x}\right\}$. Then $(x - \epsilon)^2 > x^2 - 2x\epsilon \ge y$. Since $x = \sup A$, by the Approximation Property we should be able to choose $t \in A$ with $(x - \epsilon) < t \le x$, but when $t > x - \epsilon$ we have $t^2 > (x - \epsilon)^2 > y$ so that $t \notin A$, and so we have the desired contradiction. Thus we must have $x^2 \le y$. Since $x^2 \ge y$ and $x^2 \le y$ we must have $x = y$.