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 $a < b \iff (a \leq b$ 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 $1 \leq n \in \mathbb{Z}$. If n is even then $(-1)^n = 1$ and $n \geq 2$ so that $\frac{1}{n} \leq \frac{1}{2}$, and so we have $x = (-1)^n + \frac{1}{n} = 1 + \frac{1}{n} \leq 1 + \frac{1}{2} = \frac{3}{2}$. If n is odd then $(-1)^n = -1$ and $n \geq 1$ so that $\frac{1}{n} \leq 1$, and so we have $x = (-1)^n + \frac{1}{n} = -1 + \frac{1}{n} \leq -1 + 1 = 0 \leq \frac{3}{2}$. In either case, we have $x \leq \frac{3}{2}$. Thus $x \leq \frac{3}{2}$ 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 $c \leq x$ for all $x \in A$, and in particular $c \leq (-1)^2 + \frac{1}{2} = \frac{3}{2}$. Thus $\frac{3}{2} = \sup A$.

We claim that $\inf A = -1$. Let $x \in A$, say $x = (-1)^n + \frac{1}{n}$ with $1 \leq n \in \mathbb{Z}$. Since $(-1)^n \geq -1$ 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 $c \leq -1$. Since -1 is a lower bound for A and since every lower bound c for A satisfies $c \leq -1$, it follows that $-1 = \inf A$, as claimed.

(b) Prove that for every $0 \leq y \in \mathbb{R}$ there exists a unique $0 \leq x \in \mathbb{R}$ 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 $x_1 \geq 0$ and $x_2 \geq 0$ 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 $x_1 \geq 0$ and $x_2 \geq 0$ 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 $0 \leq y \in \mathbb{R}$. Let $A = \left\{0 \leq t \in \mathbb{R} \,\middle|\, t^2 \leq y\right\}$. Note that $A \neq \emptyset$ since $0 \in A$. We claim that A is bounded above. If $0 \leq y \leq 1$ then A is bounded above by 1 because $t > 1 \implies t^2 > 1 \implies t^2 > y \implies t \notin A$. If $y \geq 1$ then A is bounded above by y because $t > y \geq 1 \implies t^2 > y^2 > y \implies t \notin A$. In either case, A is bounded above. Since $A \neq \emptyset$ 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 $0 < \epsilon \leq 1$ we have $(x + \epsilon)^2 = x^2 + 2x\epsilon + \epsilon^2 \leq x^2 + 2x\epsilon + \epsilon = x^2 + (2x + 1)\epsilon$ and we have $x^2 + (2x + 1)\epsilon \leq y \iff \epsilon \leq \frac{y - x^2}{2x+1}$. Choose $\epsilon = \min\left\{1, \frac{y-x^2}{2x+1}\right\}$. Then $(x + \epsilon)^2 \leq x^2 + (2x + 1)\epsilon \leq y$ so that $x + \epsilon \in A$, which contradicts the fact that $x = \sup A$. Thus we must have $x^2 \geq y$. Now suppose, for a contradiction, that $x^2 > y$. Note that for $0 < \epsilon \leq x$ we have $(x - \epsilon)^2 = x^2 - 2x\epsilon + \epsilon^2 > x^2 - 2x\epsilon$ and we have $x^2 - 2x\epsilon \geq y \iff \epsilon \leq \frac{x^2 - y}{2x}$. Choose $\epsilon = \min\left\{x, \frac{x^2-y}{2x}\right\}$. Then $(x - \epsilon)^2 > x^2 - 2x\epsilon \geq y$. Since $x = \sup A$, by the Approximation Property we should be able to choose $t \in A$ with $(x - \epsilon) < t \leq x$, 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 $x^2 \leq y$. Since $x^2 \geq y$ and $x^2 \leq y$ we must have $x = y$.

4: In this problem, and in the following problem, you may use any known properties of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

(a) Let X and Y be nonempty sets and let $f : X \to Y$. Prove that f is injective if and only if we have $f(A \cap B) = f(A) \cap f(B)$ for all subsets $A, B \subseteq X$.

Solution: Suppose that f is injective. Let $A, B \subseteq X$. Let $y \in f(A \cap B)$. Choose $x \in A \cap B$ with $f(x) = y$. Since $x \in A$ and $y = f(x)$ we have $y \in f(A)$. Since $x \in B$ and $y = f(x)$ we have $y \in f(B)$. Thus $y \in f(A) \cap f(B)$, showing that that $f(A \cap B) \subseteq f(A) \cap f(B)$ (we did not use the fact that f was injective). Now let $y \in f(A) \cap f(B)$. Since $y \in f(A)$ we can choose $x_1 \in A$ with $f(x_1) = y$. Since $y \in f(B)$ we can choose $x_2 \in B$ with $f(x_2) = y$. Since $f(x_1) = y = f(x_2)$ and f is injective, we must have $x_1 = x_2$, say $x_1 = x_2 = x$. Since $x = x_1 \in A$ and $x = x_2 \in B$ we have $x \in A \cap B$. Since $x \in A \cap B$ and $y = f(x_1) = f(x_2) = f(x)$ we have $y \in f(A \cap B)$, hence $f(A) \cap f(B) \subseteq f(A \cap B)$. Thus $f(A \cap B) = f(A) \cap f(B)$ for all $A, B \subseteq X$.

Suppose that f is not injective. Choose $x_1, x_2 \in X$ with $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$, and let $y = f(x_1) = f(x_2)$. Let $A = \{x_1\}$ and $B = \{x_2\}$. Then $f(A) \cap f(B) = \{y\} \cap \{y\} = \{y\}$ but $A \cap B = \{x_1\} \cap \{x_2\} = \emptyset$ so $f(A \cap B) = f(\emptyset) = \emptyset$. For these sets A, B, we do not have $f(A \cap B) = f(A) \cap f(B)$.

(b) Show that $|\mathbb{R}| = \big|[0,1)\big|$ without using the Cantor-Schröder-Bernstein Theorem.

Solution: The map $f : [0, \infty) \to [0, 1)$ given by $f(x) = \frac{x}{x+1}$ is bijective with inverse given by $f^{-1}(y) = \frac{y}{1-y}$ because for all $x \in [0, \infty)$ and all $y \in [0, 1)$ we have

$$y = \tfrac{x}{x+1} \iff xy + y = x \iff x(1-y) = y \iff x = \tfrac{y}{1-y}\,.$$

The map $g : \mathbb{N} \times [0,1) \to [0, \infty)$ given by $g(n,t) = n + t$ is bijective with inverse $g^{-1}(x) = \big(\lfloor x \rfloor\,,\, x - \lfloor x \rfloor\big)$ because for all $(n,t) \in \mathbb{N} \times [0,1)$ and all $x \in [0, \infty)$ we have

$$x = n + t \iff \big(n = \lfloor x \rfloor \text{ and } t = x - \lfloor x \rfloor\big) \iff (n,t) = \big(\lfloor x \rfloor\,,\, x - \lfloor x \rfloor\big).$$

We claim that the map $h : \mathbb{Z} \times [0,1) \to \mathbb{N} \times [0,1)$ given by

$$h(n,t) = \begin{cases} (2n, t) & \text{if } n \geq 0, \\ (-2n-1, t) & \text{if } n < 0 \end{cases}$$

is bijective with inverse $\ell : \mathbb{N} \times [0,1) \to \mathbb{Z} \times [0,1)$ given by $\ell(2j, t) = (j, t)$ and $\ell(2j+1, t) = (-j-1, t)$ for $j \in \mathbb{N}$. For $n \in \mathbb{Z}$ and $t \in [0,1)$, when $n \geq 0$ we have $\ell\big(h(n,t)\big) = \ell(2n,t) = (n,t)$ and when n is odd we have $\ell\big(h(t)\big) = \ell\big(-2n-1, t\big) = \ell\big(2(-n-1)+1\,,\, t\big) = \big(-(-n-1)\,,\, t\big) = (n,t)$. Thus $\ell(h(n,t) = (n,t)$ for all $n \in \mathbb{Z}$ and all $t \in [0,1)$, and so ℓ is a left inverse for h. For $m \in \mathbb{N}$ and $t \in [0,1)$, we can write $m = 2j$ or $m = 2j+1$ with $j \in \mathbb{N}$, and then we have $h\big(\ell(2j,t)\big) = h(j,t) = (2j,t)$ and we have $h\big(\ell((2j+1,t)\big) = h\big(-j-1, t\big) = \big(-2(-j-1)-1\,,\, t\big) = (2j+1, t)$. Thus $h\big(\ell(m,t)\big) = (m,t)$ for all $m \in \mathbb{N}$ and all $t \in [0,1)$ and so ℓ is a right inverse for h. Since ℓ is both a left inverse and a right inverse for h, it is the (two-sided) inverse of h, as claimed. Finally, the map $k : \mathbb{R} \to \mathbb{Z} \times [0,1)$ given by $k(x) = \big(\lfloor x \rfloor\,,\, x - \lfloor x \rfloor\big)$ is bijective with inverse given by $k^{-1}(n,t) = n + t$ by the same calculation which showed that g was bijective. The composite map $f \circ g \circ h \circ k$ is a bijective map from $\mathbb{R}$ to $[0,1)$ so we have $|\mathbb{R}| = \big|[0,1)\big|$, as required.

5: (a) Show that the cardinality of the set of all finite subsets of $\mathbb{N}$ is equal to $\aleph_0$.

Solution: Let A be the set of finite subsets of $\mathbb{N}$. We define a bijective map $F:\mathbb{N}\to A$ as follows. Given $n\in\mathbb{N}$ we can write n (uniquely) in its binary representation as $n=a_m a_{m-1}\cdots a_1 a_0$, so we have $n=\sum\limits_{i=0}^{m} a_i 2^i$ where each $a_i\in\{0,1\}$ with $a_m=1$ (unless $n=0$ in which case $m=a_m=0$). We then define

$$F(n)=F\Big(\sum_{k=0}^{m} a_k 2^k\Big)=\big\{k\in\mathbb{N}\big|a_k=1\big\}.$$

(for example, when $n=19$, in binary notation $n=10011$ and so $F(n)=\{0,1,4\}$). The inverse map $G:A\to\mathbb{N}$ is given by

$$G(S)=\sum_{k=0}^{\infty} a_k 2^k \text{ where } a_k=\begin{cases}1 \text{ if } k\in S,\\ 0 \text{ if } k\notin S.\end{cases}$$

In the above equation, S is a finite subset of $\mathbb{N}$, and the sum $\sum\limits_{k=0}^{\infty} a_k 2^k$ finite because S is finite so that $a_k=1$ for only finitely many values of $k\in\mathbb{N}$.

(b) Show that the cardinality of the set of all functions from $\mathbb{N}$ to $\mathbb{N}$ is equal to $2^{\aleph_0}$.

Solution: Recall that $2^{\mathbb{N}}$ denotes the set of functions from $\mathbb{N}$ to $\{0,1\}$, and $\mathbb{N}^{\mathbb{N}}$ denotes the set of functions from $\mathbb{N}$ to $\mathbb{N}$. Note that $2^{\mathbb{N}}\subseteq\mathbb{N}^{\mathbb{N}}$ (since every function from $\mathbb{N}$ to $\{0,1\}$ is also a function from $\mathbb{N}$ to $\mathbb{N}$) and so we have $|2^{\mathbb{N}}|\le|\mathbb{N}^{\mathbb{N}}|$. Recall that each element $n\in\mathbb{N}$ can be written uniquely in the form $n=2^k(2l+1)-1$ with $k,l\in\mathbb{N}$. Define $F:\mathbb{N}^{\mathbb{N}}\to 2^{\mathbb{N}}$ by

$$F(f)\big(2^k(2l+1)-1\big)=\begin{cases}1 \text{ if } k=f(l),\\ 0 \text{ if } k\neq f(l).\end{cases}$$

(In the above equation, $f:\mathbb{N}\to\mathbb{N}$ and $F(f):\mathbb{N}\to\{0,1\}$). We claim that F is injective. Let $f,g:\mathbb{N}\to\mathbb{N}$. Suppose that $F(f)=F(g)$. Then $F(f)(n)=F(g)(n)$ for all $n\in\mathbb{N}$. Given $k,l\in\mathbb{N}$, let $n=2^k(2l-1)-1$. Then we have $k=f(l)\iff F(f)(n)=1\iff F(g)(n)=1\iff k=g(l)$. Thus $f(l)=g(l)$ for all $l\in\mathbb{N}$, and so $f=g$. Thus F is injective, as claimed, and so we have $|\mathbb{N}^{\mathbb{N}}|\le|2^{\mathbb{N}}|$. By the Cantor-Schroeder-Bernstein Theorem, it follows that $|\mathbb{N}^{\mathbb{N}}|=|2^{\mathbb{N}}|$.