Homework 1 Solutions

Math 171, Spring 2010
Please send corrections to henrya@math.stanford.edu

2.2. Let $h : X \to Y$, $g : Y \to Z$, and $f : Z \to W$. Prove that $(f \circ g) \circ h = f \circ (g \circ h)$.

Solution. Let $x \in X$. Note that

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x)$$

Since this is true for all $x \in X$, we have $(f \circ g) \circ h = f \circ (g \circ h)$.

2.3. Let $f : X \to Y$ and $A \subset X$ and $B \subset Y$. Prove (a) $f(f^{-1}(B)) \subset B$ and (b) $A \subset f^{-1}(f(A))$.

Solution. (a) By definition, $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$. So if $y \in f(f^{-1}(B))$, then $y = f(x)$ for some $x \in f^{-1}(B)$, that is, $f(x) \in B$. Hence $y = f(x) \in B$, so $f(f^{-1}(B)) \subset B$.

(b) If $x \in A$, then $f(x) \in f(A)$, and so $x \in f^{-1}(f(A))$. Hence $A \subset f^{-1}(f(A))$.

3.3. Prove that $-(-x) = x$ for all $x \in \mathbb{R}$.

Solution. Note that $x + (-x) = 0 = (-x) + x$, by definition of $(-x)$. By the uniqueness in Axiom 5, x is the additive inverse of $(-x)$, that is, $-(-x) = x$.

3.5. Let $x, y \in \mathbb{R}$. Prove that $xy = 0$ if and only if $x = 0$ or $y = 0$.

Solution. To show $\Leftarrow$, suppose that either $x = 0$ or $y = 0$. Then, by Theorem 3.4, $xy = 0$.

To show $\Rightarrow$, let $xy = 0$. Suppose for a contradiction that $x \neq 0$ and $y \neq 0$. Since x and y are nonzero, by Axiom 10 their multiplicative inverses x^{-1} and y^{-1} exist. Hence we have

$$0 = 0(y^{-1}x^{-1}) = (xy)(y^{-1}x^{-1}) = xx^{-1} = 1$$

This contradicts Axiom 9, which says $0 \neq 1$. Hence it must be the case that either $x = 0$ or $y = 0$. This shows $\Rightarrow$.

We have $xy = 0 \Leftrightarrow x = 0$ or $y = 0$.

4.4. Prove that if $xy > 0$, then either $x > 0$ and $y > 0$ or $x < 0$ and $y < 0$, $x, y \in \mathbb{R}$.

Solution. Let $xy > 0$. By Exercise 3.5, $x \neq 0$ and $y \neq 0$.

If $x > 0$ and $y < 0$, then Theorem 4.2 says $xy < 0y = 0$, a contradiction.

If $x < 0$ and $y > 0$, then Theorem 4.2 says $0 = 0y > xy$, a contradiction.

Hence it must be the case that $x > 0$ and $y > 0$ or $x < 0$ and $y < 0$.

4.7. Prove that $x^2 + y^2 \geq 2xy$ for all $x, y \in \mathbb{R}$.

Solution. Note $(x - y)^2 \geq 0$. Expanding, we get $x^2 - 2xy + y^2 \geq 0$. Adding $2xy$ to both sides, we get $x^2 + y^2 \geq 2xy$.

5.1. Let X be a set of real numbers with least upper bound a. Prove that if $\epsilon > 0$, there exists $x \in X$ such that $a - \epsilon < x \leq a$.

Solution. Suppose for a contradiction that there is no such x. Then $a - \epsilon$ is an upper bound for X, and $a - \epsilon < a$. This contradicts the fact that a is the least upper bound for X: see part (ii) of Definition 5.2. Hence there must exist some $x \in X$ such that $a - \epsilon < x \leq a$.

5.7. Let X and Y be sets of real numbers with least upper bounds a and b, respectively. Prove that $a+b$ is the least upper bound of the set $X + Y = \{x + y \mid x \in X, y \in Y\}$.

Solution. First note that if $z \in X + Y$, then $z = x + y$ with $x \in X$ and $y \in Y$, so $z = x + y \leq a + b$. Hence $a + b$ is an upper bound for $X + Y$.

Next, let c be any upper bound for $X + Y$. Suppose for a contradiction that $c < a + b$. Let $\epsilon = a + b - c > 0$. By Exercise 5.1, there exists $x \in X$ such that $a - \frac{\epsilon}{2} < x$, and there exists $y \in Y$ such that $b - \frac{\epsilon}{2} < y$. Hence $c = a + b - \epsilon = (a - \frac{\epsilon}{2}) + (b - \frac{\epsilon}{2}) < x + y$, contradicting the fact that c is an upper bound for $X + Y$. So it must be that $a + b \leq c$.

Thus $a + b$ is the least upper bound of $X + Y$.

6.3. Prove the binomial theorem: If a and b are real numbers and n is a positive integer, then

$$(a+b)^n = \binom{n}{0}a^n + \dots + \binom{n}{k}a^{n-k}b^k + \dots + \binom{n}{n}b^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Solution. This is a proof by induction on n. The base case when $n = 1$ is clear, as $\binom{1}{0} = 1 = \binom{1}{1}$.

For the inductive step, assume it holds for m. Then for $n = m + 1$,

$$\begin{aligned}
(a+b)^{m+1} &= (a+b)(a+b)^m \\
&= (a+b)(a^m + b^m + \sum_{k=1}^{m-1}\binom{m}{k}a^{m-k}b^k) \text{ by the inductive hypothesis} \\
&= a^{m+1} + b^{m+1} + ab^m + ba^m + \sum_{k=1}^{m-1}\binom{m}{k}a^{m-k+1}b^k + \sum_{k=1}^{m-1}\binom{m}{k}a^{m-k}b^{k+1} \\
&= a^{m+1} + b^{m+1} + \sum_{k=1}^{m}\binom{m}{k}a^{m-k+1}b^k + \sum_{k=0}^{m-1}\binom{m}{k}a^{m-k}b^{k+1} \text{ by combining terms} \\
&= a^{m+1} + b^{m+1} + \sum_{k=1}^{m}\binom{m}{k}a^{m-k+1}b^k + \sum_{j=1}^{m}\binom{m}{j-1}a^{m+1-j}b^j \text{ let j=k+1 in second sum} \\
&= a^{m+1} + b^{m+1} + \sum_{k=1}^{m}\left[\binom{m}{k} + \binom{m}{k-1}\right]a^{m+1-k}b^k \text{ by combining the sums} \\
&= a^{m+1} + b^{m+1} + \sum_{k=1}^{m}\binom{m+1}{k}a^{m+1-k}b^k \text{ from Pascal's rule} \\
&= \sum_{k=0}^{m+1}\binom{m+1}{k}a^{m+1-k}b^k
\end{aligned}$$

as desired. Hence the binomial theorem holds for all positive integers n.

6.4. Prove that if X is a nonempty subset of positive integers which is bounded above, then X contains a greatest element.

Solution. Since X is bounded above, there exists $b \in \mathbb{P}$ such that $x < b$ for all $x \in X$. Hence $b - x \in \mathbb{P}$ for all $x \in X$. By Theorem 6.10, there exists a least element in the nonempty set $\{b - x : x \in X\}$ of positive integers. That is, there exists some $y \in X$ such that $b - y \leq b - x$ for all $x \in X$. Subtracting b from both sides and multiplying by -1, we get that $y \geq x$ for all $x \in X$. Hence X contains a greatest element y.

7.5. Prove the laws of integer exponents

Solution.

(a) $x^{m+n} = x^m x^n,\ x \in \mathbb{R},\ x \neq 0,\ m, n \in \mathbb{Z}$

Definition 7.3 tells us that $x^{n+1} = xx^n$ (and hence $x^{-1}x^{n+1} = x^n$) for all $n \in \mathbb{P}$. First we show this is true for all $n \in \mathbb{Z}$. The cases $n = 0, -1$ are clear. Also, if $n < -1$, then we have

$$x^{n+1} = \frac{1}{x^{-n-1}} = \frac{1}{x^{-1}x^{-n}} = \frac{1}{x^{-1}}\frac{1}{x^{-n}} = xx^n$$

Hence $x^{n+1} = xx^n$ for all $n \in \mathbb{Z}$.

Now, let $m \in \mathbb{Z}$ be arbitrary. We will show that $x^{m+n} = x^m x^n$ by induction on n. The base case $n = 0$ is clear. Suppose the formula is true for n. Then

$$x^{m+n+1} = xx^{m+n} = xx^m x^n = x^m x^{n+1}$$

so the formula is true for $n + 1$. This shows the formula is true for all $n \in \mathbb{N}$. Suppose again the formula is true for n. Then

$$x^{m+n-1} = x^{-1}x^{m+n} = x^{-1}x^m x^n = x^m x^{n-1}$$

so the formula is true for $n - 1$. Hence the formula is true for all $n \in \mathbb{Z}$.

(b) $x^n = \frac{1}{x^{-n}},\ x \in \mathbb{R},\ x \neq 0,\ n \in \mathbb{Z}$.

If $n \leq 0$, then this is Definition 7.3. If $n > 0$, then note $\frac{1}{x^{-n}} = \frac{1}{\frac{1}{x^n}} = x^n$.

(c) $(xy)^n = x^n y^n,\ x, y \in \mathbb{R},\ x \neq 0 \neq y,\ n \in \mathbb{Z}$.

We prove the formula by induction on n. The base case $n = 0$ is clear. Suppose the formula is true for n. Then

$$(xy)^{n+1} = (xy)(xy)^n = xyx^n y^n = x^{n+1}y^{n+1}$$

so the formula is true for $n + 1$. This shows the formula is true for all $n \in \mathbb{N}$. Suppose again the formula is true for n. Then

$$(xy)^{n-1} = (xy)^{-1}(xy)^n = x^{-1}y^{-1}x^n y^n = x^{n-1}y^{n-1}$$

so the formula is true for $n - 1$. Hence the formula is true for all $n \in \mathbb{Z}$.

(d) $(x^m)^n = x^{mn},\ x \in \mathbb{R},\ x \neq 0,\ m, n \in \mathbb{Z}$

Let $m \in \mathbb{Z}$ be arbitrary. We prove the formula by induction on n. The base case $n = 0$ is clear. Suppose the formula is true for n. Then

$$(x^m)^{n+1} = (x^m)(x^m)^n = x^m x^{mn} = x^{m+mn} = x^{m(n+1)}$$

so the formula is true for $n + 1$. This shows the formula is true for all $n \in \mathbb{N}$. Suppose again the formula is true for n. Then

$$(x^m)^{n-1} = (x^m)^{-1}(x^m)^n = x^{-m}x^{mn} = x^{-m+mn} = x^{m(n-1)}$$

so the formula is true for $n - 1$. Hence the formula is true for all $n \in \mathbb{Z}$.

(e) $(\frac{x}{y})^n = \frac{x^n}{y^n},\ x, y \in \mathbb{R},\ x \neq 0 \neq y,\ n \in \mathbb{Z}$.

This follows by replacing y with y^{-1} in (b).

(f) If $0 < x < y$, then $x^n < y^n,\ n \in \mathbb{P}$

We prove the formula by induction on n. The base case $n = 1$ is clear. Suppose the formula is true for n. Then

$$x^{n+1} = xx^n < xy^n < yy^n = y^{n+1}$$

so the formula is true for $n+1$. This shows the formula is true for all $n \in \mathbb{P}$.

(g) If $n < m$ and $x > 1$, then $x^n < x^m,\ n, m \in \mathbb{Z}$.

Let $n \in \mathbb{Z}$ be arbitrary. We prove the formula by induction on m. The base case $m = n+1$ is clear, as $1 < x$ implies

$$x^n < xx^n = x^{n+1} = x^m$$

Suppose the formula is true for m. Then

$$x^n < x^m < xx^m = x^{m+1}$$

so the formula is true for $m+1$. This shows the formula is true for all $m > n$.

7.10. Prove that no equilateral triangle in the plane can have all vertices with rational coordinates.

Solution. Suppose for a contradiction that such a triangle exists. Translate the triangle so that one vertex is at the origin; note the new vertices still have rational coordinates. Scale the triangle by the common denominator of the new rational coordinates to produce an equilateral triangle with integer coordinates. Let these coordinates be $(0, 0)$, (a, b), and (c, d).

Let s be the common length of each side. We have

$$s^2 = a^2 + b^2 = c^2 + d^2 = (a-c)^2 + (b-d)^2$$

Expanding the right hand side gives

$$s^2 = (a^2 + b^2) + (c^2 + d^2) - 2(ac + bd)$$

so $2(ac + bd) = s^2$. So

$$4(ac + bd)^2 = s^4 = (a^2 + b^2)(c^2 + d^2)$$

Expanding gives

$$4(ac)^2 + 8abcd + 4(bd)^2 = (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2$$

Canceling like terms and rearranging gives

$$3(ac + bd)^2 = (ad - bc)^2$$

The integer on the left hand side has an odd number of threes in its prime factorization, whereas the integer on the right has an even number of threes, which contradicts unique factorization of integers into primes. Hence no equilateral triangle in the plane can have all vertices with rational coordinates. (Note: this argument using uniqueness of prime factorization to show a contradiction above is essentially the same as the argument showing $\sqrt{3}$ is irrational.)

8.3. Prove that every infinite set has a countably infinite subset.

Solution. Let X be an infinite set. Since X is nonempty, there exists some $x_1 \in X$. Note that $X \setminus \{x_1\}$ is nonempty, for otherwise X would be a finite set. Hence there exists some $x_2 \in X \setminus \{x_1\}$. For the inductive step, suppose that we have chosen $\{x_1, ..., x_n\} \subset X$ (with the x_i disjoint). Note that $X \setminus \{x_1, ..., x_n\}$ is nonempty, for otherwise X would be a finite set. Hence there exists some $x_{n+1} \in X \setminus \{x_1, ..., x_n\}$. By induction, we have constructed a countably infinite subset $\{x_1, x_2, x_3, ...\}$ of X.

8.5. Let X be a set. Let S be the set of all functions from X into $\{0, 1\}$. Prove that $S \approx P(X)$. How does this exercise connect Example 8.3 and Corollary 8.5?

Solution. Define $f : S \to P(X)$ as follows. Given $s \in S$, let $f(s) = \{x \in X : s(x) = 1\}$. Note that f is one-to-one, for if $f(s) = f(s')$, then $\{x \in X : s(x) = 1\} = \{x \in X : s'(x) = 1\}$, and so $s = s'$. Also, f is onto, for if $Y \in P(X)$, then define $s_Y \in S$ by $s_Y(x) = 1$ if $x \in Y$ and $s_Y(x) = 0$ otherwise, and note that $f(s_Y) = Y$. So f is a one-to-one function from S onto $P(X)$, giving $S \approx P(X)$.

Let $X = \mathbb{P}$, so S is the set of all functions from $\mathbb{P}$ into $\{0,1\}$, that is, the set of all real sequences which assume only the values 0 or 1. By this exercise, $S \approx P(\mathbb{P})$. So S is uncountable if and only if $P(\mathbb{P})$ is uncountable. Hence, Example 8.3 and this exercise imply Corollary 8.5. Vice-versa, Corollary 8.5 and this exercise imply Example 8.3.