# Math 430 – Problem Set 1 Solutions

Due January 22, 2016

1.2. If $A = \{a, b, c\}, B = \{1, 2, 3\}, C = \{x\}$, and $D = \varnothing$, list all of the elements of each of the following sets.

(a) $A \times B$

**Solution.**

$$\{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}.$$

(b) $B \times A$

**Solution.**

$$\{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c)\}.$$

(c) $A \times B \times C$

**Solution.**

$$\{(a, 1, x), (a, 2, x), (a, 3, x), (b, 1, x), (b, 2, x), (b, 3, x), (c, 1, x), (c, 2, x), (c, 3, x)\}.$$

(d) $A \times D$

**Solution.**

$$\emptyset.$$

Note that $\{\emptyset\}$ is not correct: this is the set containing $\emptyset$.

1.6. Prove $(A \cup B) \cap (A \cup C) = A \cup (B \cap C)$.

**Solution.** Suppose $x \in A \cup (B \cap C)$. Then, either $x \in A$ (case 1) or $x \in B \cap C$ (case 2). Since $A \subseteq A \cup B$ and $A \subseteq A \cup C$, in case 1 we get that $x \in A \cup B$ and $x \in A \cup C$ and thus $x \in (A \cup B) \cap (A \cup C)$. In case 2, since $x \in B$ and $B \subseteq A \cup B$, we know $x \in A \cup B$. Similarly, since $x \in C$ and $C \subseteq A \cup C$, we know $x \in (A \cup C)$. So in both cases, $x \in (A \cup B) \cap (A \cup C)$ and therefore $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Conversely, suppose $x \in (A \cup B) \cap (A \cup C)$. If $x \in A$, then $x \in A \cup (B \cap C)$. Alternatively, if $x \notin A$ then $x$ must be in $B$ and in $C$ since $x \in (A \cup B)$ and $x \in (A \cup C)$. Thus $x \in (B \cap C)$. Therefore $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. With both inclusions proven, we get $(A \cup B) \cap (A \cup C) = A \cup (B \cap C)$. □

1.17. Which of the following relations $f : \mathbb{Q} \to \mathbb{Q}$ define a mapping? In each case, supply a reason why $f$ is or is not a mapping.

(a) $f(p/q) = \frac{p+1}{p-2}$

**Solution.** Note that $1/2 = 3/6$, but $f(1/2) = -2$ while $f(3/6) = 4$. Since $f$ is multivalued, it is not a function.

(b) $f(p/q) = \frac{3p}{3q}$

**Solution.** This is a function. If $p/q = p'/q'$ then $\frac{3p}{3q} = \frac{p}{q} = \frac{p'}{q'} = \frac{3p'}{3q'}$.

(c) $f(p/q) = \frac{p+q}{q^2}$

**Solution.** Note that $1/2 = 2/4$, but $f(1/2) = \frac{3}{4}$ while $f(2/4) = \frac{6}{16}$. Since $f$ is multivalued, it is not a function.

(d) $f(p/q) = \frac{3p^2}{7q^2} - \frac{p}{q}$

**Solution.** This is a function. If $p/q = p'/q'$ then $pq' = qp'$. Thus

$$\begin{aligned} f(p/q) &= \frac{3p^2}{7q^2} - \frac{p}{q} \\ &= \frac{3p^2(q')^2}{7q^2(q')^2} - \frac{p'}{q'} \\ &= \frac{3(pq')^2}{7q^2(q')^2} - \frac{p'}{q'} \\ &= \frac{3(p'q)^2}{7q^2(q')^2} - \frac{p'}{q'} \\ &= \frac{3(p')^2q^2}{7(q')^2q^2} - \frac{p'}{q'} \\ &= \frac{3(p')^2}{7(q')^2} - \frac{p'}{q'} \\ &= f(p'/q'). \end{aligned}$$

1.20. (a) Define a function $f : \mathbb{N} \to \mathbb{N}$ that is one-to-one but not onto.

**Solution.** The function $f(n) = n + 1$ is one-to-one (if $n + 1 = m + 1$ then $n = m$) but not onto (1 is not in the image since $0 \notin \mathbb{N}$).

(b) Define a function $f : \mathbb{N} \to \mathbb{N}$ that is onto but not one-to-one.

**Solution.** The function $f(n) = \lceil n/2 \rceil$ is onto (given $m$, $f(2m) = m$) but not one-to-one ($f(1) = f(2) = 1$).

1.22. Let $f : A \to B$ and $g : B \to C$ be maps.

(a) If $f$ and $g$ are both one-to-one functions, show that $g \circ f$ is one-to-one.

**Solution.** Suppose $a, a' \in A$ with $g(f(a)) = g(f(a'))$. Since $g$ is one-to-one, $f(a) = f(a')$. Since $f$ is one-to-one, $a = a'$. Thus $g \circ f$ is one-to-one. $\square$

(b) If $g \circ f$ is onto, show that $g$ is onto.

**Solution.** Suppose $c \in C$. Since $g \circ f$ is onto, there is an $a \in A$ with $g(f(a)) = c$. Setting $b = f(a)$, we have $b \in B$ with $g(b) = c$. Thus $g$ is onto. $\square$

(c) If $g \circ f$ is one-to-one, show that $f$ is one-to-one.

**Solution.** Suppose that $a, a' \in A$ with $f(a) = f(a')$. Then $g(f(a)) = g(f(a'))$. Since $g \circ f$ is one-to-one, $a = a'$. Thus $f$ is one-to-one. $\square$

(d) If $g \circ f$ is one-to-one and $f$ is onto, show that $g$ is one-to-one.

**Solution.** By (c), $f$ is one-to-one and thus bijective. Therefore it has an inverse, so $g = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1}$ is the composition of one-to-one functions and is thus one-to-one. $\square$

(e) If $g \circ f$ is onto and $g$ is one-to-one, show that $f$ is onto.

**Solution.** One can argue as in part (d), or as follows. Suppose $b \in B$. Since $g \circ f$ is onto, there is an $a \in A$ with $g(f(a)) = g(b)$. Since $g$ is one-to-one, $f(a) = b$. Thus $f$ is onto. $\square$

1.25. Determine whether or not the following relations are equivalence relations on the given set. If the relation is an equivalence relation, describe the partition given by it. If the relation is not an equivalence relation, state why it fails to be one.

(a) $x \sim y$ in $\mathbb{R}$ if $x \geq y$

**Solution.** This relation is not an equivalence relation since it is not symmetric: $2 \sim 1$ but $1 \not\sim 2$.

(b) $m \sim y$ in $\mathbb{Z}$ if $mn > 0$

**Solution.** This relation is not an equivalence relation since it is not reflexive: $0 \not\sim 0$.

(c) $x \sim y$ in $\mathbb{R}$ if $|x - y| \leq 4$

**Solution.** This relation is not an equivalence relation since it is not transitive: $0 \sim 3$ and $3 \sim 6$ but $0 \not\sim 6$.

(d) $m \sim n$ in $\mathbb{Z}$ if $m \equiv n \pmod 6$

**Solution.** This relation is an equivalence relation. The partition are the congruence classes modulo 6: $0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}, 4 + 6\mathbb{Z}$ and $5 + 6\mathbb{Z}$.

1.28. Find the error in the following argument by providing a counterexample. "The reflexive property is redundant in the axioms for an equivalence relation. If $x \sim y$, then $y \sim x$ by the symmetric property. Using the transitive property, we can deduce that $x \sim x$."

**Solution.** The problem is that, given $x$, there may be no $y$ with $x \sim y$. For example, for any set $X$, consider the empty relation where $x \sim y$ is never true. This is symmetric and transitive, but not reflexive.

2.9. Use induction to prove that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for $n \in \mathbb{N}$.

**Solution.** For the base case of $n = 1$, we have $1 + 2 = 2^2 - 1$.

Suppose that $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$. Then

$$\begin{aligned} 1 + 2 + 2^2 + \cdots + 2^{n-1} + 2^n &= (2^n - 1) + 2^n \\ &= 2 \cdot 2^n - 1 \\ &= 2^{n+1} - 1. \end{aligned}$$

The result then holds by induction. □

2.12. For every positive integer $n$, show that a set with exactly $n$ elements has a power set with exactly $2^n$ elements.

**Solution.** We prove this statement by induction. If $X = \{x\}$ has one element, then $\mathcal{P}(X) = \{\emptyset, \{x\}\}$ has two elements and the base case holds.

Now assume that the statement holds for a given positive integer $n$. Let $X = \{a_1, \ldots, a_{n+1}\}$ have $n+1$ elements. Let

$$\begin{aligned} P_{\text{in}} &= \{A \in \mathcal{P}(X) \mid a_{n+1} \in A\} \\ P_{\text{out}} &= \{A \in \mathcal{P}(X) \mid a_{n+1} \notin A\} \end{aligned}$$

Since every $A \in \mathcal{P}(X)$ either contains $a_{n+1}$ or does not, $\mathcal{P}(X) = P_{\text{in}} \sqcup P_{\text{out}}$ is a disjoint union of $P_{\text{in}}$ and $P_{\text{out}}$ and thus the number of elements in $\mathcal{P}(X)$ is the sum of the sizes of $P_{\text{in}}$ and of $P_{\text{out}}$. Since $P_{\text{out}} = \mathcal{P}(\{a_1, \ldots, a_n\})$, it has $2^n$ elements by the induction hypothesis. The function

$$\begin{aligned} P_{\text{out}} &\to P_{\text{in}} \\ A &\mapsto A \cup \{a_{n+1}\} \end{aligned}$$

is a bijection, and thus $P_{\text{in}}$ and $P_{\text{out}}$ have the same size. Therefore, $\mathcal{P}(X)$ has size $2^n + 2^n = 2^{n+1}$. □

2.15(b). Find $d = \gcd(234, 165)$ and integers $r$ and $s$ with $d = 234r + 165s$.

**Solution.** Running the Euclidean algorithm,

$$\begin{aligned}
234 &= 1 \cdot 165 + 69 \\
165 &= 2 \cdot 69 + 27 \\
69 &= 2 \cdot 27 + 15 \\
27 &= 1 \cdot 15 + 12 \\
15 &= 1 \cdot 12 + 3 \\
12 &= 4 \cdot 3,
\end{aligned}$$

so the greatest common divisor is 3. Now

$$\begin{aligned}
3 &= 15 - 12 \\
&= 15 - (27 - 15) \\
&= 2 \cdot 15 - 27 \\
&= 2 \cdot (69 - 2 \cdot 27) - 27 \\
&= 2 \cdot 69 - 5 \cdot 27 \\
&= 2 \cdot 69 - 5 \cdot (165 - 2 \cdot 69) \\
&= 12 \cdot 69 - 5 \cdot 165 \\
&= 12 \cdot (234 - 165) - 5 \cdot 165 \\
&= 12 \cdot 234 - 17 \cdot 165,
\end{aligned}$$

so we may take $r = 12$ and $s = -17$.

2.17(e). Prove that $f_n$ and $f_{n+1}$ are relatively prime.

**Solution.** We prove this statement by induction. Since $\gcd(1, 1) = 1$, the base case holds: $f_1$ and $f_2$ are relatively prime.

Suppose that $f_{n-1}$ and $f_n$ are relatively prime: $\gcd(f_{n-1}, f_n) = 1$. Then

$$\begin{aligned}
\gcd(f_{n+1}, f_n) &= \gcd(f_{n-1} + f_n, f_n) \\
&= \gcd(f_{n-1}, f_n) \\
&= 1,
\end{aligned}$$

as in one step of the Euclidean algorithm. The result then holds by induction. $\square$

2.30. Prove that there are an infinite number of primes of the form $4n - 1$.

**Solution.** Suppose, for contradiction, that there are finitely many: $p_1, \ldots, p_k$. Let $N = 4p_1 \ldots p_k - 1$. Since $N$ differers from a multiple of every $p_i$ by 1, it cannot be divisible by any $p_i$ on the list. But it also cannot be divisible only by primes of the form $4n + 1$ since the product of such primes will be congruent to 1 modulo 4, while $N \equiv -1 \pmod 4$. Moreover, $N$ is odd so it is not divisible by any even prime. Thus $N$ must be divisible by at least one prime of the form $4n - 1$ that does not show up on the initial list. This contradiction proves the result. $\square$

2.31. Using the fact that 2 is prime, show that there do not exist integers $p$ and $q$ such that $p^2 = 2q^2$. Demonstrate that therefore $\sqrt{2}$ cannot be a rational number.

**Solution.** Suppose that there are integers $p$ and $q$ with $p^2 = 2q^2$. Among such pairs, chose the one with the smallest positive value of $p$. Since 2 is prime and divides $p^2$, it must in fact divide $p$ and thus $p = 2m$. Then $q^2 = 2m^2$, so $(q, m)$ also provides a solution. Since $q < p$, this contradicts the minimality of $p$.

If $\sqrt{2} = \frac{p}{q}$ is rational, squaring both sides and multiplying by $q^2$ yields $p^2 = 2q^2$, which we just showed was impossible. $\square$