Mathematics 216
Robert Gross
Homework 26
Answers

1. Let $f : X \to Y$ be a function. Suppose that for all subsets $A, B \subset X$, we know that $f(A \cap B) = f(A) \cap f(B)$. Prove or give a counterexample:

(a) f must be a surjection.

(b) f must be an injection.

Answer: (a) This is *false*. Consider $X = \{1\}$, $Y = \{1, 2\}$, and $f(1) = 1$. The function is not surjective, but because the only subsets of X are X and $\emptyset$, we can verify that $f(A \cap B) = f(A) \cap f(B)$ for all $A, B \subset X$.

(b) This is *true*. Suppose that $f(x_1) = f(x_2)$. We need to prove that $x_1 = x_2$. Let $A = \{x_1\}$ and $B = \{x_2\}$. We are given $f(A \cap B) = f(A) \cap f(B)$. We know that $f(A) \cap f(B) = \{f(x_1)\}$. Therefore, $A \cap B \neq \emptyset$, because $f(\emptyset) = \emptyset$. If $A \cap B \neq \emptyset$, we must have $A = B$ and then $x_1 = x_2$.

2. Let $M_2(\mathbf{R})$ be the set of all 2×2-matrices with real entries. Define a relation on $M_2(\mathbf{R})$ by saying that the matrices A and B are *similar* if there is an invertible matrix T so that $AT = TB$. Show that similarity of matrices is an equivalence relation.

Answer: We check the usual 3 properties:

- *Reflexivity*: Pick $A \in M_2(\mathbf{R})$. The identity matrix I is invertible, and we know that $AI = IA$. Therefore, A is similar to itself.
- *Symmetry*: Suppose $A, B \in M_2(\mathbf{R})$, with A similar to B. That means that $AT = TB$ for some invertible matrix T. Multiply that equation by T^{-1} on both the left and right and we get $BT^{-1} = T^{-1}A$. Because T^{-1} is also an invertible matrix, we conclude that B is similar to A.
- *Transitivity*: Suppose $A, B, C \in M_2(\mathbf{R})$, with A similar to B and B similar to C. This means that there is an invertible matrix T so that $AT = TB$ and another invertible matrix S so that $BS = SC$. Therefore, $A(TS) = (AT)S = (TB)S = T(BS) = T(SC) = (TS)C$. Because both T and S are invertible, we know that TS is invertible, and therefore A is similar to C.

3. Suppose that n is an integer which is at least 2, a an integer which is relatively prime to n, and $k = o([a]_n)$. Prove that $o([a^d]_n) = k/(k, d)$.

Answer: We know that $(a^d)^{k/(k,d)} \equiv (a^k)^{d/(k,d)} \equiv 1^{d/(k,d)} \equiv 1 \pmod{n}$, so $o([a^d]_n) \leq k/(k, d)$.

Now, suppose that $(a^d)^j \equiv 1 \pmod{n}$, with $j > 0$. We need to show that $j \geq k/(k, d)$. We have $a^{dj} \equiv 1 \pmod{n}$, and therefore $o(a) | dj$, or $k | dj$. Divide by (k, d), and we have $\frac{k}{(k,d)} | \frac{d}{(k,d)} j$. Now, $k/(k, d)$ and $d/(k, d)$ are relatively prime, and therefore we know that $\frac{k}{(k,d)} | j$. This says that $\frac{k}{(k,d)} \leq j$, which is the desired result.

4. Suppose that n is an integer which is at least 2, and a and b are integers which are each relatively prime to n. Suppose that $o([a]_n) = k$, and $o([b]_n) = j$, and $(k, j) = 1$. Prove that $o([ab]_n) = jk$.

Answer: We know that $(ab)^{kj} \equiv (a^k)^j (b^j)^k \equiv 1^j 1^k \equiv 1 \pmod{n}$. This shows that $o(ab) \leq kj$.

Now, suppose that $m > 0$ and $(ab)^m \equiv 1 \pmod{n}$. We need to prove that $m \geq kj$.

First, raise the equation to the power k, and we get $a^{km}b^{km} \equiv 1 \pmod{n}$. Because $a^k \equiv 1 \pmod{n}$, we have $b^{km} \equiv 1 \pmod{n}$, and hence $o(b)|km$. Because $(j,k) = 1$, we have $j|m$.

Second, raise the equation to the power j, and we get $a^{jm}b^{jm} \equiv 1 \pmod{n}$. Because $b^j \equiv 1 \pmod{n}$, we have $a^{jm} \equiv 1 \pmod{n}$. Hence $o(a)|jm$. Because $(k,j) = 1$, we have $k|m$.

Finally, we have $j|m$, $k|m$, and $(j,k) = 1$, which combine to tell us that $jk|m$, and hence $jk \leq m$.

5. Suppose that D is an integral domain. Define a relation $\sim$ on $D \times (D \setminus \{0\})$ with the formula $(a,b) \sim (c,d)$ if $ad = bc$. Prove that the relation $\sim$ is transitive.

Answer: Suppose that $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. That gives $ad = bc$ and $cf = de$. Multiply the first equation by f to get $adf = bcf$. Multiply the second equation by b to get $bcf = bde$. Therefore, $adf = bde$. Now, because $d \neq 0$, we can cancel d and get $af = be$, which says that $(a,b) \sim (e,f)$.

6. Now define a relation $\sim$ on $\mathbf{Z}/20\mathbf{Z} \times (\mathbf{Z}/20\mathbf{Z} \setminus \{0\})$ with the same formula: $(a,b) \sim (c,d)$ if $ad = bc$. Show that $\sim$ is *not* transitive.

Answer: We have $(0,1) \sim (0,5)$, and $(0,5) \sim (4,5)$, but $(0,1) \not\sim (4,5)$.