

CS1231S: Discrete Structures
Tutorial #6: Functions
(Week 8: 5 – 9 October 2026)
Answers

1. Define the following relations on $\mathbb{N}$:

$$\forall x, y \in \mathbb{N} (x R_1 y \Leftrightarrow x^2 = y^2);$$

$$\forall x, y \in \mathbb{N} (x R_2 y \Leftrightarrow y \mid x);$$

$$\forall x, y \in \mathbb{N} (x R_3 y \Leftrightarrow y = x + 1).$$

Are the relations R_1 , R_2 and R_3 functions? Prove or disprove.

Answers:

R_1 is a function.

Proof:

(F1) $\forall x \in \mathbb{N}, \exists y = x \in \mathbb{N}$ such that $(x, y) \in R_1$.

- (F2)
1. $\forall x \in \mathbb{N}$, let $y_1, y_2 \in \mathbb{N}$.
 2. Suppose $(x, y_1) \in R_1 \wedge (x, y_2) \in R_1$.
 3. Then $y_1^2 = x^2$ and $y_2^2 = x^2$ (by the definition of R_1).
 4. Then $y_1^2 = y_2^2$.
 5. Hence $y_1 = y_2$ (as $y_1, y_2 \in \mathbb{N} \geq 0$).

R_2 is not a function. Counterexample: $(6 R_2 2) \wedge (6 R_2 3)$.

R_3 is a function.

Proof:

(F1) $\forall x \in \mathbb{N}, \exists y = x + 1 \in \mathbb{N}$ such that $(x, y) \in R_3$.

- (F2)
1. $\forall x \in \mathbb{N}$, let $y_1, y_2 \in \mathbb{N}$.
 2. Suppose $(x, y_1) \in R_3 \wedge (x, y_2) \in R_3$.
 3. Then $y_1 = x + 1$ and $y_2 = x + 1$ (by the definition of R_3).
 4. Hence $y_1 = y_2$.

A **function** $f: X \rightarrow Y$, is a relation satisfying the following properties:

(F1) $\forall x \in X, \exists y \in Y$ such that $(x, y) \in f$.

(F2) $\forall x \in X, \forall y_1, y_2 \in Y, ((x, y_1) \in f \wedge (x, y_2) \in f) \rightarrow y_1 = y_2$.

2. Let $A = \{s, u\}$. Define a function $\text{len}: A^* \rightarrow \mathbb{Z}_{\geq 0}$ by setting $\text{len}(\sigma)$ to be the length of σ for each $\sigma \in A^*$.
- What is $\text{len}(suu)$?
 - What is $\text{len}(\{\epsilon, ss, uu, ssss\})$?
 - What is $\text{len}^{-1}(\{3\})$?
 - Does len^{-1} exist? Explain your answer.

Answers:

- $\text{len}(suu) = 3$.
- $\text{len}(\{\epsilon, ss, uu, ssss\}) = \{0, 2, 4\}$.
- $\text{len}^{-1}(\{3\}) = \{sss, ssu, sus, suu, uss, usu, uus, uuu\}$.
- $\text{len}(s) = 1 = \text{len}(u)$ but $s \neq u$. So len is not injective and so it is not bijective. Thus len^{-1} does not exist by **Theorem 7.2.3**. (Recall that len^{-1} refers to the inverse function of len .)

Theorem 7.2.3

If $f: X \rightarrow Y$ is a bijection, then $f^{-1}: Y \rightarrow X$ is also a bijection. In other words, $f: X \rightarrow Y$ is bijective iff f has an inverse.

3. Given any two bijections $f: A \rightarrow B$ and $g: B \rightarrow C$, prove that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Answer:

- Since f and g are bijections, f^{-1} and g^{-1} are bijections by **theorem 7.2.3**, and $g \circ f$ and $f^{-1} \circ g^{-1}$ are also bijection by **theorems 7.3.3 and 7.3.4**.
- Since $g \circ f$ is a bijection, $(g \circ f)^{-1}$ exists and is a bijection by **theorem 7.2.3**.
- (To check the domains and codomains of $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$.)
 - Domain and codomain of $g \circ f$ are A and C respectively, hence domain and codomain of $(g \circ f)^{-1}$ are C and A respectively.
 - Domain and codomain of f^{-1} are B and A respectively, domain and codomain of g^{-1} are C and B respectively, hence domain and codomain of $f^{-1} \circ g^{-1}$ are C and A respectively.
 - Therefore, $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$ have the same domain and codomain.
- (To check that $(g \circ f)^{-1}(z)$ and $f^{-1} \circ g^{-1}(z)$ have the same image for all $z \in C$.)
 - Let $z \in C$.
 - Then $\exists y \in B$ such that $z = g(y)$, or $y = g^{-1}(z)$ by **definition of inverse function**.
 - Similarly, $\exists x \in A$ such that $y = f(x)$, or $x = f^{-1}(y)$ by **definition of inverse function**.
 - Hence $(g \circ f)(x) = g(f(x)) = g(y) = z$, or $(g \circ f)^{-1}(z) = x$ by **definition of inverse function**.
 - Also, $(f^{-1} \circ g^{-1})(z) = f^{-1}(g^{-1}(z)) = f^{-1}(y) = x$.
 - Therefore, $(g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$ for all $z \in C$ from **lines 4.4 and 4.5**.
- Therefore, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ from **3 and 4**.

Theorem 7.2.3

If $f: X \rightarrow Y$ is a bijection, then $f^{-1}: Y \rightarrow X$ is also a bijection.

Theorem 7.3.3

If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both injective, then $g \circ f$ is injective.

Theorem 7.3.4

If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both surjective, then $g \circ f$ is surjective.

4. Which of the functions defined in the following are injective? Which are surjective? Prove that your answers are correct. If a function defined below is both injective and surjective, then find a formula for the inverse of the function. Here we denote by *Bool* the set {**true**, **false**}.

- (a) $f: \mathbb{Q} \rightarrow \mathbb{Q};$
 $x \mapsto 12x + 31.$
- (b) $g: Bool^2 \rightarrow Bool;$
 $(p, q) \mapsto p \wedge \sim q.$
- (c) $h: Bool^2 \rightarrow Bool^2;$
 $(p, q) \mapsto (p \wedge q, p \vee q).$
- (d) $k: \mathbb{Z} \rightarrow \mathbb{Z};$
 $x \mapsto \begin{cases} x, & \text{if } x \text{ is even;} \\ 2x - 1, & \text{if } x \text{ is odd.} \end{cases}$

Inverse function

Let $f: X \rightarrow Y$. Then $g: Y \rightarrow X$ is an **inverse** of f iff
 $\forall x \in X \forall y \in Y (y = f(x) \Leftrightarrow x = g(y)).$

Answers:

(a) We could prove that f is injective and surjective, and hence bijective. Here, we try another approach: if we manage to find an inverse function for f , then by **Theorem 7.2.3**, f is bijective.

- Note that for all $x, y \in \mathbb{Q}, y = 12x + 31 \Leftrightarrow x = (y - 31)/12$.
- Define $f^*: \mathbb{Q} \rightarrow \mathbb{Q}$ by setting, for all $y \in \mathbb{Q}, f^*(y) = (y - 31)/12$.
- Then whenever $x, y \in \mathbb{Q}, y = f(x) \Leftrightarrow x = f^*(y)$.
- Thus f^* is the inverse of f .
- Hence f is **bijective** (i.e. both injective and surjective) by **Theorem 7.2.3**.

(b)

- $g(\text{false}, \text{true}) = \text{false} = g(\text{false}, \text{false})$, where $(\text{false}, \text{true}) \neq (\text{false}, \text{false})$.
- So g is **not injective**.
- $g(\text{true}, \text{false}) = \text{true}$.
- Lines 1 and 3 show that every element of the codomain *Bool* is in the range of g .
- Hence g is **surjective**.

(c)

- $h(\text{true}, \text{false}) = (\text{false}, \text{true}) = g(\text{false}, \text{true})$, where $(\text{true}, \text{false}) \neq (\text{false}, \text{true})$.
- So h is **not injective**.
- If $p, q, r \in Bool$ such that $h(p, q) = (\text{true}, r)$, then
 - $p \wedge q = \text{true}$ by the definition of h ;
 - $\therefore p = \text{true}$
 - $\therefore r = p \vee q = \text{true}$ by the definition of h .
- So $(\text{true}, \text{false})$ in the codomain is not in the range of h .
- Hence h is **not surjective**.

(d)

1. We first show that if x is an even integer, then $k(x)$ is even.
 - 1.1. Let x be an even integer.
 - 1.2. Then $k(x) = x$ by the definition of k .
 - 1.3. So $k(x)$ is even.
2. Next we show that if x is an odd integer, then $k(x)$ is odd.
 - 2.1. Let x be an odd integer.
 - 2.2. Then $k(x) = 2x - 1 = 2(x - 1) + 1$, where $x - 1$ is an integer.
 - 2.3. So $k(x)$ is odd.
3. Since every integer is either even or odd but not both, lines 1 and 2 tell us that, for every $x \in \mathbb{Z}$,
 - 3.1. x is even if and only if $k(x)$ is even; and
 - 3.2. x is odd if and only if $k(x)$ is odd.
4. Now we show that k is injective.
 - 4.1. Let $x_1, x_2 \in \mathbb{Z}$ such that $k(x_1) = k(x_2)$.
 - 4.2. Case 1: $k(x_1)$ is even.
 - 4.2.1. Then both x_1 and x_2 are even by line 3.1.
 - 4.2.2. So $x_1 = k(x_1) = k(x_2) = x_2$ by the definition of k .
 - 4.3. Case 2: $k(x_1)$ is odd.
 - 4.3.1. Then both x_1 and x_2 are odd by line 3.2.
 - 4.3.2. So $2x_1 - 1 = k(x_1) = k(x_2) = 2x_2 - 1$ by the definition of k .
 - 4.3.3. So $x_1 = x_2$.
 - 4.4. Since $k(x_1)$ is either even or odd, we conclude that $x_1 = x_2$ in any case.
 - 4.5. Therefore k is injective.
5. Finally, we prove by contradiction that k is not surjective.
 - 5.1. Suppose k is surjective.
 - 5.2. Note that 3 is in the codomain $\mathbb{Z}$.
 - 5.3. Use the surjectivity of k to find $x \in \mathbb{Z}$ such that $k(x) = 3$.
 - 5.4. Note that $k(x) = 3$ is odd and so x is odd by line 3.2.
 - 5.5. Thus $3 = k(x) = 2x - 1$ by the choice of x and the definition of k .
 - 5.6. Solving gives $x = \frac{3+1}{2} = 2$ which is even.
 - 5.7. This contradicts line 5.4 that x is odd.
 - 5.8. Therefore k is not surjective.

5. [AY2022/23 Semester 2 Exam Questions]

The following definitions are given.

Given a function $f: A \rightarrow B$, we say that

- $g: B \rightarrow A$ is a **left inverse** of f if and only if $g(f(a)) = a$ for all $a \in A$.
- $h: B \rightarrow A$ is a **right inverse** of f if and only if $f(h(b)) = b$ for all $b \in B$.

You do not need to provide proofs for the following parts.

- (a) Which of the 4 functions given in question 4 have a left inverse?
- (b) Which of the 4 functions given in question 4 have a right inverse?
- (c) Which of the following statements are true?
 - (i) If a function has a left inverse, then it has a right inverse.
 - (ii) If a function has a right inverse, then it has a left inverse.

Answers:

- (a) Only f and k . (b) Only f and g . (c) Neither is true.

Note that

- a function is injective if and only if it has a left inverse;
- a function is surjective if and only if it has a right inverse.

6. We have shown in Theorem 7.3.3 that if $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both injective, then $g \circ f$ is injective.

Now, let $f: B \rightarrow C$. Suppose we have a function g with domain C such that $g \circ f$ is injective. Show that f is injective.

Answer:

1. Suppose g is a function with domain C such that $g \circ f$ is injective.
2. Let $x_1, x_2 \in B$ such that $f(x_1) = f(x_2)$.
3. Then $(g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2)$ by the definition of $g \circ f$.
4. So $x_1 = x_2$ as $g \circ f$ is injective by the choice of g .
5. Therefore f is injective.

7. Let $A = \{1, 2, 3\}$. The **order** of a bijection $f: A \rightarrow A$ is defined to be the smallest $n \in \mathbb{Z}^+$ such that

$$\underbrace{f \circ f \circ \cdots \circ f}_{n\text{-many } f\text{'s}} = id_A.$$

Define functions $g, h: A \rightarrow A$ by setting, for all $x \in A$,

$$g(x) = \begin{cases} 1, & \text{if } x = 2; \\ 2, & \text{if } x = 1; \\ x, & \text{otherwise,} \end{cases} \quad h(x) = \begin{cases} 2, & \text{if } x = 3; \\ 3, & \text{if } x = 2; \\ x, & \text{otherwise.} \end{cases}$$

Find the orders of $g, h, g \circ h$, and $h \circ g$.

Answers: The orders for $g, h, g \circ h$, and $h \circ g$ are 2, 2, 3 and 3 respectively.

$$(g \circ g)(1) = g(g(1)) = g(2) = 1$$

$$(g \circ g)(2) = g(g(2)) = g(1) = 2$$

$$(g \circ g)(3) = g(g(3)) = g(3) = 3$$

Therefore $g \circ g$ is an identity function on A . Hence $g \circ g$ has an order of 2.

Similar working for h .

Let $s = g \circ h$.

$$s(1) = (g \circ h)(1) = g(h(1)) = g(1) = 2$$

$$s(2) = (g \circ h)(2) = g(h(2)) = g(3) = 3$$

$$s(3) = (g \circ h)(3) = g(h(3)) = g(2) = 1$$

$$(s \circ s \circ s)(1) = s(s(s(1))) = s(s(2)) = s(3) = 1$$

$$(s \circ s \circ s)(2) = s(s(s(2))) = s(s(3)) = s(1) = 2$$

$$(s \circ s \circ s)(3) = s(s(s(3))) = s(s(1)) = s(2) = 3$$

Therefore $(g \circ h) \circ (g \circ h) \circ (g \circ h)$ is an identity function on A . Hence $g \circ h$ has an order of 3.

Similar working for $h \circ g$.

8. [AY2023/24 Semester 2 Exam Questions]

Recall Theorem 4.4.1 (The Quotient-Remainder Theorem):

“Given any integer n and positive integer d , there exist unique integers q and r such that $n = dq + r$ and $0 \leq r < d$.”

Definitions:

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Suppose $n = dq + r$ and $0 \leq r < d$, we define $n \% d = r$.

Given a function $f(x)$, we define the function $f^{(n)}(x)$ to be the result of n applications of f to x , where $n \in \mathbb{Z}^+$. For example, $f^{(3)}(x) = f(f(f(x)))$. We also define the **order** of an input x with respect to f to be the smallest positive integer m such that $f^{(m)}(x) = x$.

Define a function $g : A \rightarrow A$ by setting, for each $x \in A$, $g(x) = 3x \% 5$.

- (a) What is $g^{(3)}(21)$?
- (b) What is the order of 3 with respect to the function g ?
- (c) Let $A = \{0,1,2,3,4\}$. Define the relation R on A as follows:

$x R y$ iff the order of x is equal to the order of y with respect to the function g .

R is an equivalence relation. Write out all the distinct equivalence classes of R using set-roster notation. Do not use the $[]$ notation.

Answers:

- (a) $g^{(3)}(21) = g^{(2)}(3) = g(4) = 2$
- (b) $g^{(4)}(3) = g^{(3)}(4) = g^{(2)}(2) = g(1) = 3$. Therefore, order of 3 is 4.
- (c) 2 equivalence classes: $\{0\}$ and $\{1, 2, 3, 4\}$.

9. Let $f: A \rightarrow B$ be a function. Let $X \subseteq A$ and $Y \subseteq B$. Justify your answers for the following:
- (a) Is it always the case that $X \subseteq f^{-1}(f(X))$? Is it always the case that $f^{-1}(f(X)) \subseteq X$?
- (b) Is it always the case that $Y \subseteq f(f^{-1}(Y))$? Is it always the case that $f(f^{-1}(Y)) \subseteq Y$?

Note that $f(X)$ is the **(setwise) image** of X , and $f^{-1}(Y)$ the **(setwise) preimage** of Y under f , where $X \subseteq A$ and $Y \subseteq B$. Without the colored font to disambiguate the two kinds of functions, it should also be clear what $f(U)$ denotes, depending on whether $U \in A$ or $U \in P(A)$.

Let $f: X \rightarrow Y$ be a function from set X to set Y .

- If $A \subseteq X$, then let $f(A) = \{f(x) : x \in A\}$.
- If $B \subseteq Y$, then let $f^{-1}(B) = \{x \in X : f(x) \in B\}$

We call $f(A)$ the **(setwise) image** of A , and $f^{-1}(B)$ the **(setwise) preimage** of B under f .

Answers:

- (a) First, we show it is always the case that $X \subseteq f^{-1}(f(X))$.

1. Let $x \in X$.
2. Then $f(x) \in f(X)$ by the definition of $f(X)$.
3. So $x \in f^{-1}(f(X))$ by the definition of $f^{-1}(f(X))$.

Next, we show it is possible that $f^{-1}(f(X)) \not\subseteq X$.

1. Consider $f: \{-1, 1\} \rightarrow \{0\}$ where $f(-1) = 0 = f(1)$, and $X = \{1\}$.
2. Note that $f(X) = \{f(1)\} = \{0\}$.
3. Since $f(-1) = 0$, we know $-1 \in f^{-1}(\{0\}) = f^{-1}(f(X))$.
4. As $-1 \notin \{1\} = X$, we deduce that $f^{-1}(f(X)) \not\subseteq X$.

(Other counterexamples are possible.)

- (b) First, we show it is always the case that $f(f^{-1}(Y)) \subseteq Y$.

1. Take any $y \in f(f^{-1}(Y))$.
2. Then we have some $x \in f^{-1}(Y)$ such that $y = f(x)$, by the definition of $f(f^{-1}(Y))$.
3. Now, as $x \in f^{-1}(Y)$, we get $y' \in Y$ which makes $y' = f(x)$.
4. Since f is a function, this implies $y = f(x) = y' \in Y$ as required.

Next, we show it is possible that $Y \not\subseteq f(f^{-1}(Y))$.

1. Consider $f: \{0\} \rightarrow \{-1, 1\}$ where $f(0) = 1$, and $Y = \{-1\}$.
2. Note that no $x \in \{0\}$ makes $f(x) = -1$.
3. So $f^{-1}(Y) = \emptyset$ by the definition of $f^{-1}(Y)$.
4. This entails $f(f^{-1}(Y)) = \emptyset \not\subseteq \{-1\} = Y$.

(Other counterexamples are possible.)

10. Consider the equivalence relation $\sim$ on $\mathbb{Q}$ defined by setting, for all $x, y \in \mathbb{Q}$,

$$x \sim y \Leftrightarrow x - y \in \mathbb{Z}.$$

Define addition and multiplication on $\mathbb{Q}/\sim$ as follows: whenever $[x], [y] \in \mathbb{Q}/\sim$,

$$[x] + [y] = [x + y] \quad \text{and} \quad [x] \cdot [y] = [x \cdot y].$$

(a) Is $+$ well defined on $\mathbb{Q}/\sim$?

(b) Is $\cdot$ well defined on $\mathbb{Q}/\sim$?

Prove that your answers are correct.

Answers:

Lemma Rel.1 Equivalence Classes

Let $\sim$ be an equivalence relation on a set A . The following are equivalent for all $x, y \in A$.

- (i) $x \sim y$; (ii) $[x] = [y]$; (iii) $[x] \cap [y] \neq \emptyset$.

(a) We claim that $+$ is well defined on $\mathbb{Q}/\sim$.

1. Let $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Q}/\sim$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.
2. So $x_1 \sim x_2$ and $y_1 \sim y_2$ by Lemma Rel.1.
3. Use the definition of $\sim$ to find $k, l \in \mathbb{Z}$ such that $x_1 - x_2 = k$ and $y_1 - y_2 = l$.
4. Note that $(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = k + l \in \mathbb{Z}$.
5. So $x_1 + y_1 \sim x_2 + y_2$ by the definition of $\sim$.
6. Hence $[x_1] + [y_1] = [x_1 + y_1] = [x_2 + y_2] = [x_2] + [y_2]$ by Lemma Rel.1.

(b) We claim that $\cdot$ is not well defined on $\mathbb{Q}/\sim$.

1. Note that $\frac{1}{2} - \frac{-1}{2} = 1 \in \mathbb{Z}$.
2. This implies $\frac{1}{2} \sim \frac{-1}{2}$ and so $\left[\frac{1}{2}\right] = \left[\frac{-1}{2}\right]$ by Lemma Rel.1.
3. Note that $\frac{1}{4} - \frac{-1}{4} = \frac{1}{2} \notin \mathbb{Z}$.
4. This implies $\frac{1}{4} \not\sim \frac{-1}{4}$ and so $\left[\frac{1}{4}\right] \neq \left[\frac{-1}{4}\right]$ by Lemma Rel.1.
5. Therefore, according to the definition of $\cdot$ on $\mathbb{Q}/\sim$,

$$\left[\frac{1}{2}\right] \cdot \left[\frac{1}{2}\right] = \left[\frac{1}{2} \cdot \frac{1}{2}\right] = \left[\frac{1}{4}\right] \neq \left[\frac{-1}{4}\right] = \left[\frac{1}{2} \cdot \frac{-1}{2}\right] = \left[\frac{1}{2}\right] \cdot \left[\frac{-1}{2}\right].$$