

Sets, Relations, and Functions

Note: Throughout this exercise set, $\mathbb{N} = \{1, 2, 3, \dots\}$ is the set of positive integers. If ρ is an equivalence relation on a set A , we denote by A/ρ the set of equivalence classes of ρ . Often A/ρ is specified by picking a unique representative from each equivalence class. We also often make use of the fact (without proof) that between every two distinct real numbers, no matter how close they are, there is always a rational number.

1. Let A, B, C be three arbitrary sets such that $A \cup B = A \cup C$ and $A \cap B = A \cap C$. Prove that $B = C$.

Solution $B = B \cap (A \cup B) = B \cap (A \cup C) = (B \cap A) \cup (B \cap C) = (A \cap C) \cup (B \cap C) = (A \cup B) \cap C = (A \cup C) \cap C = C$.

You can alternatively use the following proof.

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

2. Define a relation ρ on \mathbb{N} as $a \rho b$ if and only if a has the same set of prime divisors as b . For example, 5 is related to $25 = 5^2$, $12 = 2^2 \times 3$ is related to $54 = 2 \times 3^3$, but 12 is not related to $16 = 2^4$, nor to $180 = 2^2 \times 3^2 \times 5$.

- (a) Prove that ρ is an equivalence relation on \mathbb{N} .

Solution [Reflexive] a has the same set of prime divisors as itself, that is, ρ is reflexive.

[Symmetric] If a has the same set of prime divisors as b , then b too has the same set of prime divisors as a , that is, ρ is symmetric.

[Transitive] If a and b have the same set of prime divisors, and b and c have the same set of prime divisors, then a and c too have the same set of prime divisors, that is, ρ is transitive.

- (b) Find a unique representative from each equivalence class of ρ .

Solution A non-zero integer is called *square-free* if it is not divisible by the square of a prime number. Each equivalence class of ρ contains a unique square-free integer, and these unique square-free integers are different in distinct equivalence classes. To see why, let $a \in \mathbb{N}$ have the prime factorization $a = p_1^{e_1} \cdots p_t^{e_t}$ with $t \geq 0$, with pairwise distinct primes p_1, \dots, p_t and with each $e_i > 0$. But then $[a] = [p_1 \cdots p_t]$. Moreover, two different square-free integers have different sets of prime divisors. So we can take square-free integers as the representatives of the equivalence classes.

3. Define two relations ρ and σ on \mathbb{R} as follows.

- (a) $a \rho b$ if and only if $a - b \in \mathbb{Q}$

- (b) $a \sigma b$ if and only if $a - b \in \mathbb{Z}$

Prove that ρ and σ are equivalence relations on \mathbb{R} . Also, find the equivalence classes (with representatives).

Solution [Reflexive] $0 = \frac{0}{1}$ is a rational (also an integer).

[Symmetric] If $a - b$ is rational (or integer), then $b - a = -(a - b)$ is rational (or integer) too.

[Transitive] If $a - b$ and $b - c$ are rational (or integer), then $a - c = (a - b) + (b - c)$ is again rational (or integer).

- (a) Equivalence classes $[x]$ of \mathbb{R}/ρ are of the form $[x] = \{x + r \mid r \in \mathbb{Q}\}$

- (b) Equivalence classes $[y]$ of \mathbb{R}/σ are of the form $[y] = \{y + s \mid s \in \mathbb{Z}\}$

We can choose a unique element in the interval $[0, 1)$ as a representative of each equivalence class of σ . For ρ however, identifying representatives in a mathematically rigorous way is not possible. If you assume the axiom of choice, then all you can say is that a unique representative from each equivalence class can be chosen. Such a choice of unique representatives from the equivalence classes gives us a set called a *Vitali set*.

4. [Genesis of rational numbers] Define a relation ρ on $A = \mathbb{Z} \times \mathbb{N}$ as $(a, b) \rho (c, d)$ if and only if $ad = bc$. Prove that ρ is an equivalence relation. Argue that A/ρ is essentially the set \mathbb{Q} of rational numbers. In abstract algebra, we say that \mathbb{Q} is the field of fractions of the integral domain \mathbb{Z} . The equivalence class $[(a, b)]$ is conventionally denoted by $\frac{a}{b}$.

Solution [Reflexive] $(a, b) \rho (a, b)$, since $ab = ba$.

[Symmetric] $(a, b) \rho (c, d)$ implies $(c, d) \rho (a, b)$, since $ad = bc \Rightarrow cb = da$.

[Transitive] Let $(a, b) \rho (c, d)$, that is, $ad = bc$, and let $(c, d) \rho (e, f)$, that is, $cf = de$. Then we get $ad = bc \Rightarrow adf = bcf \Rightarrow adf = bde \Rightarrow af = be$ (since $d \neq 0$), that is, $(a, b) \rho (e, f)$.

Equivalence classes of A/ρ are of the form $[(a, b)] = \frac{a}{b} = \left\{ \frac{na}{nb} \mid n \in \mathbb{N} \right\}$. A unique representative from each equivalence class can be chosen as $\frac{a}{b}$ with $\gcd(a, b) = 1$.

5. For a function $f : A \rightarrow B$, define a function $\mathcal{F} : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ as $\mathcal{F}(S) = f(S)$ for all $S \subseteq A$, where $\mathcal{P}(A)$ and $\mathcal{P}(B)$ denote the power sets of A and B , respectively. (Earlier, we have denoted \mathcal{F} by f , but now we need a new name for it.) Prove the following.

- (a) \mathcal{F} is injective if and only if f is injective.

Solution For $S \subseteq A$, we have $\mathcal{F}(S) = f(S) = \{f(a) \mid a \in S\}$.

[\Rightarrow] Let $f(a_1) = f(a_2)$ for $a_1, a_2 \in A$. We have $\mathcal{F}(\{a_1\}) = \{f(a_1)\}$ and $\mathcal{F}(\{a_2\}) = \{f(a_2)\}$, that is, $\mathcal{F}(\{a_1\}) = \mathcal{F}(\{a_2\})$. Since \mathcal{F} is injective, this implies that $\{a_1\} = \{a_2\}$, that is, $a_1 = a_2$.

[\Leftarrow] Take $S_1, S_2 \in \mathcal{P}(A)$ with $\mathcal{F}(S_1) = \mathcal{F}(S_2)$. We need to show $S_1 = S_2$. Take $a_1 \in S_1$. Then $b = f(a_1) \in \mathcal{F}(S_1)$. But then, since $\mathcal{F}(S_1) = \mathcal{F}(S_2)$, there exists $a_2 \in S_2$ such that $b = f(a_2)$, that is, $f(a_1) = f(a_2)$. Since f is injective, we have $a_1 = a_2$, that is, $a_1 \in S_2$. This proves that $S_1 \subseteq S_2$. Likewise, $S_2 \subseteq S_1$. Therefore $S_1 = S_2$.

- (b) \mathcal{F} is surjective if and only if f is surjective.

Solution [\Rightarrow] Take $b \in B$. Since \mathcal{F} is surjective, there exists $S \in \mathcal{P}(A)$ such that $\mathcal{F}(S) = \{b\}$. Since $\mathcal{F}(\emptyset) = \emptyset$, we conclude that $S \neq \emptyset$. But then, for any $a \in S$, we have $f(a) = b$.

[\Leftarrow] Take any $T \in \mathcal{P}(B)$. Since f is surjective, we can say that for any $b \in T$, there exists $a_b \in A$ such that $f(a_b) = b$. Take $S = \{a_b \mid b \in T\}$. It is easy to see that $f(S) = T$.

6. Let $f : A \rightarrow B$ be a function, and σ an equivalence relation on B . Define a relation ρ on A as: $a \rho a'$ if and only if $f(a) \sigma f(a')$.

- (a) Prove that ρ is an equivalence relation on A .

Solution Let $a, a', a'' \in A$.

[ρ is reflexive] Clearly, $f(a) \sigma f(a)$ (since σ is reflexive), that is, $a \rho a$.

[ρ is symmetric] Let $a \rho a'$. By definition, $f(a) \sigma f(a')$, that is, $f(a') \sigma f(a)$ (σ is symmetric), so $a' \rho a$.

[ρ is transitive] Let $a \rho a'$ and $a' \rho a''$. By definition, $f(a) \sigma f(a')$ and $f(a') \sigma f(a'')$, that is, $f(a) \sigma f(a'')$ (since σ is transitive), that is, $a \rho a''$.

- (b) Define a map $\bar{f} : A/\rho \rightarrow B/\sigma$ as $[a]_\rho \mapsto [f(a)]_\sigma$. Prove that \bar{f} is well-defined.

Solution Suppose $[a]_\rho = [a']_\rho$, that is, $a \rho a'$. By definition, $f(a) \sigma f(a')$, that is, $[f(a)]_\sigma = [f(a')]_\sigma$.

- (c) Prove that \bar{f} is injective.

Solution Suppose $\bar{f}([a]_\rho) = \bar{f}([a']_\rho)$, that is, $[f(a)]_\sigma = [f(a')]_\sigma$, that is, $f(a) \sigma f(a')$, that is, $a \rho a'$, that is, $[a]_\rho = [a']_\rho$. So \bar{f} is injective.

(Remark: This proof never demands f to be injective.)

- (d) Prove or disprove: If f is a bijection, then so also is \bar{f} .

Solution This is true. By Part (c), \bar{f} is injective. On the other hand, take any $[b]_\sigma \in B/\sigma$. Since f is surjective, we have $b = f(a)$ for some $a \in A$. But then $\bar{f}([a]_\rho) = [f(a)]_\sigma = [b]_\sigma$, that is, \bar{f} is surjective too.

(Remark: We never used the fact that f is injective. Indeed, \bar{f} is bijective, whenever f is surjective.)

- (e) Prove or disprove: If \bar{f} is a bijection, then so also is f .

Solution This is false. Take $A = \{a, b, c\}$, $B = \{1, 2\}$ and $\sigma = \{(1, 1), (2, 2)\}$. Also define f as $f(a) = f(b) = 1$ and $f(c) = 2$. Then $\rho = \{(a, a), (b, b), (a, b), (b, a), (c, c)\}$, that is, $A/\rho = \{\{a, b\}, \{c\}\}$, $B/\sigma = \{\{1\}, \{2\}\}$, and $\bar{f}(\{a, b\}) = \{1\}$ and $\bar{f}(\{c\}) = \{2\}$. Therefore, \bar{f} is a bijection, whereas f is not.

7. Give an example of a poset A and a non-empty subset S of A such that S has lower bounds in A , but $\text{glb}(S)$ does not exist.

Solution Take $A = \mathbb{Q}$ under the standard \leq on rational numbers. Also take $S = \{x \in \mathbb{Q} \mid x^2 > 2\}$. Every rational number $< \sqrt{2}$ is a lower bound on S . Since $\sqrt{2}$ is irrational, $\text{glb}(S)$ does not exist.

Another example: Take A to be the set of all irrational numbers between 1 and 5, and S to be the set of all irrational numbers between 2 and 3.

A simpler (but synthetic) example: Take $A = \{a, b, c, d\}$ and the relation on A as,

$$\rho = \{(a, a), (a, c), (a, d), (b, b), (b, c), (b, d), (c, c), (d, d)\}$$

The subset $S = \{c, d\}$ of A has two lower bounds a and b , but these bounds are not comparable to one another.

8. Let $k \in \mathbb{N}$, $S = \{1, 2, \dots, k\}$, and $A = \mathcal{P}(S) \setminus \{\emptyset\}$, where $\mathcal{P}(S)$ denotes the power set of S . In other words, the set A consists of all non-empty subsets of $\{1, 2, \dots, k\}$. For each $a \in A$, denote by $\min(a)$ the smallest element of a (notice that here a is a set).

- (a) Define a relation ρ on A as follows: $a \rho b$ if and only if $\min(a) = \min(b)$. Prove that ρ is an equivalence relation on A .

Solution [Reflexive] For any $a \in A$ we have $\min(a) = \min(a)$.

[Symmetric] For any $a, b \in A$, if $\min(a) = \min(b)$, then $\min(b) = \min(a)$.

[Transitive] For any $a, b, c \in A$, if $\min(a) = \min(b)$ and $\min(b) = \min(c)$, then $\min(a) = \min(c)$.

- (b) What is the size of the quotient set A/ρ ?

Solution Any two non-empty subsets of S having the same minimum element are related. On the other hand, two subsets of S having different minimum elements are not related. Therefore, the equivalence classes of ρ have a one-to-one correspondence with elements of S (the minimum element of every member in the class). Since S contains k elements, there are exactly k equivalence classes, that is, the size of A/ρ is k .

- (c) Define a relation σ on A as follows: $a \sigma b$ if and only if either $a = b$ or $\min(a) < \min(b)$. Prove that, σ is a partial order on A .

Solution [Reflexive] By definition, every element is related to itself.

[Antisymmetric] Take two elements $a, b \in A$. Suppose that $a \sigma b$ and $b \sigma a$. If $a \neq b$, then by definition, $\min(a) < \min(b)$ and $\min(b) < \min(a)$, which is impossible. So we must have $a = b$.

[Transitive] Suppose $a \sigma b$ and $b \sigma c$ for some $a, b, c \in A$. If $a = b$ or $b = c$, then clearly $a \sigma c$. So suppose that $a \neq b$ and $b \neq c$. But then, $\min(a) < \min(b)$ and $\min(b) < \min(c)$. This implies that $\min(a) < \min(c)$, that is, $a \sigma c$.

- (d) Is σ also a total order on A ?

Solution No! Take $k > 2$. The sets $\{1\}$ and $\{1, 2\}$ are distinct, but have the same minimum element, and are therefore not comparable.

9. Let A be a lattice with respect to a relation \preceq . Prove that every non-empty finite subset of S has a least upper bound and a greatest lower bound.

Solution Let S be a non-empty finite subset of A with $|S| = n$. We prove by induction on n that $\text{lub}(S)$ exists. A proof for the existence of $\text{glb}(S)$ proceeds analogously.

Since $S \neq \emptyset$, we have $n \geq 1$. For $n = 1, 2$, the assertion about the existence of $\text{lub}(S)$ is obvious. So take $n \geq 3$, and assume that every $(n-1)$ - and $(n-2)$ -element subset of A has a least upper bound. Take $S = \{a_1, a_2, \dots, a_n\} \subseteq A$. Since A is a lattice, $b = \text{lub}(a_{n-1}, a_n)$ exists. Let $T = \{a_1, a_2, \dots, a_{n-2}, b\}$. By the induction hypothesis, T has a least upper bound (T has size $n-1$ or $n-2$).

Let U_S (resp. U_T) be the set of all upper bounds of S (resp. T). We first claim that $U_S = U_T$. For the proof, first take $u \in U_S$. Then $a_i \preceq u$ for all $i = 1, 2, \dots, n$. In particular, $a_{n-1} \preceq u$ and $a_n \preceq u$. Since $b = \text{lub}(a_{n-1}, a_n)$, we

have $b \preceq u$, that is, $u \in U_T$. Conversely, if $u \in U_T$, then $a_i \preceq u$ for all $i = 1, 2, \dots, n-2$, and $b \preceq u$. Since b is an upper bound of both a_{n-1} and a_n , we also have $a_{n-1} \preceq b$ and $a_n \preceq b$. By transitivity, $a_{n-1} \preceq u$ and $a_n \preceq u$. Thus $u \in U_S$.

Since T has a least upper bound, U_T is non-empty and contains the unique minimum element $\text{lub}(T)$. Since $U_S = U_T$, the same conclusions apply to S as well. It therefore follows that $\text{lub}(S) = \text{lub}(T)$.

(Remark: The above result applies only to finite subsets of A . Infinite subsets may have no least upper bounds and/or no greatest lower bounds. For example, consider the divisibility lattice on \mathbb{N} . The lcm of any finite (and non-zero) number of elements exists, but the lcm of an infinite number of (distinct) elements does not exist.)

Additional Exercises

10. Let $f : A \rightarrow B$ be a function. Prove the following assertions.

- (a) $S \subseteq f^{-1}(f(S))$ for every $S \subseteq A$. Give an example where the inclusion is proper.
- (b) f is injective if and only if $S = f^{-1}(f(S))$ for every $S \subseteq A$.
- (c) $f(f^{-1}(T)) \subseteq T$ for every $T \subseteq B$. Give an example where the inclusion is proper.
- (d) f is surjective if and only if $f(f^{-1}(T)) = T$ for every $T \subseteq B$.
- (e) $f(f^{-1}(f(S))) = f(S)$ for all $S \subseteq A$.
- (f) $f^{-1}(f(f^{-1}(T))) = f^{-1}(T)$ for all $T \subseteq B$.

11. Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be functions.

- (a) Prove that if the function $g \circ f : A \rightarrow C$ is injective, then f is injective.
- (b) Give an example in which $g \circ f$ is injective, but g is not injective.
- (c) Prove that if $g \circ f$ is surjective, then g is surjective.
- (d) Give an example in which $g \circ f$ is surjective, but f is not surjective.

12. A function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ is called *nilpotent* if for some $n \in \mathbb{N}$ we have $f^n(a) = 0$ for all $a \in \mathbb{Z}$.

- (a) Prove or disprove: The function $f(a) = \lfloor a/2 \rfloor$ is nilpotent.
- (b) Give an example of a non-constant nilpotent function.

* 13. A function $f : \mathbb{R} \rightarrow \mathbb{R}$ is called *monotonic increasing* if $f(a) \leq f(b)$ whenever $a \leq b$. It is called *strictly monotonic increasing* if $f(a) < f(b)$ whenever $a < b$. One can define *monotonic decreasing* and *strictly monotonic decreasing* functions in analogous ways.

- (a) Prove that a strictly monotonic increasing function is injective.
- (b) Demonstrate that an injective function $\mathbb{R} \rightarrow \mathbb{R}$ need not be strictly increasing or strictly decreasing.
- (c) Prove that a continuous injective function $\mathbb{R} \rightarrow \mathbb{R}$ is either strictly increasing or strictly decreasing.

14. Let A be the set of all functions $\mathbb{R} \rightarrow \mathbb{R}$. Define relations ρ, σ, τ on A as follows: (i) $f \rho g$ if and only if $f(a) \leq g(a)$ for all $a \in \mathbb{R}$; (ii) $f \sigma g$ if and only if $f(0) \leq g(0)$; (iii) $f \tau g$ if and only if $f(0) = g(0)$. Argue which of the relations ρ, σ, τ is/are equivalence relation(s). Argue which is/are partial order(s).

15. Let ρ be a relation on a set A . Define $\rho^{-1} = \{(b, a) \mid (a, b) \in \rho\}$. Also for two relations ρ, σ on A , define the composite relation $\rho \circ \sigma$ as $(a, c) \in \rho \circ \sigma$ if and only if there exists $b \in A$ such that $(a, b) \in \rho$ and $(b, c) \in \sigma$. Prove the following assertions.

- (a) ρ is both symmetric and antisymmetric if and only if $\rho \subseteq \{(a, a) \mid a \in A\}$.
- (b) ρ is transitive if and only if $\rho \circ \rho = \rho$.
- (c) If ρ is non-empty, then ρ is an equivalence relation if and only if $\rho^{-1} \circ \rho = \rho$.
- (d) ρ is a partial order if and only if ρ^{-1} is a partial order.

16. Let A be the set of all non-empty finite subsets of \mathbb{Z} . Define a relation ρ on A as: $U \rho V$ if and only if $\min(U) = \min(V)$. Also define the relation σ on A as: $U \sigma V$ if and only if $\min(U) \leq \min(V)$. Finally, define a relation τ on A as: $U \tau V$ if and only if either $U = V$ or $\min(U) < \min(V)$.

- (a) Prove that ρ is an equivalence relation on A .
- (b) Identify good representatives from the equivalence classes of ρ .
- (c) Define a bijection between the quotient set A/ρ and \mathbb{Z} .
- (d) Prove or disprove: σ is a partial order on A .
- (e) Prove or disprove: τ is a partial order on A .

17. Let $f : A \rightarrow B$ be a function, ρ an equivalence relation on A , and σ an equivalence relation on B . Suppose further that if $f(a) \sigma f(a')$, then $a \rho a'$. Show by an explicit example that the association $\bar{f} : A/\rho \rightarrow B/\sigma$ given by $\bar{f}([a]_\rho) = [f(a)]_\sigma$ is not necessarily a function.
18. Let m, n be positive integers. Prove that the assignment $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ taking $[a]_m \mapsto [a]_n$ is well-defined if and only if m is an integral multiple of n . (**Remark:** \mathbb{Z}_n is the set of all equivalence classes of congruence modulo n . The equivalence class of $a \in \mathbb{Z}$ is denoted by $[a]_n$. We can take unique representatives from the classes to define \mathbb{Z}_n as $\{0, 1, 2, \dots, n-1\}$.)
19. A *string* is a finite ordered sequence of symbols from a finite alphabet. We start with a predetermined total ordering of the alphabet, and then define the usual dictionary order on strings. For example, if the alphabet is $\{a, b, c\}$, and we take the ordering $a \leq b \leq c$, then we have $a \leq aa \leq aba \leq abca \leq b \leq bacb \leq bbca \leq c \leq ca$. Prove that this dictionary order (called *lexicographic ordering*) is a total ordering.
20. Define a relation \leq_{DL} on $A = \mathbb{N} \times \mathbb{N}$ as follows. Take $(a, b), (c, d) \in A$ and call $(a, b) \leq_{DL} (c, d)$ if either (i) $a + b < c + d$, or (ii) $a + b = c + d$ and $a \leq c$.
- Prove that \leq_{DL} is a partial order on A .
 - Prove that \leq_{DL} is a total order on A .
 - Prove or disprove: An infinite subset of A may contain a maximum element.
- Note:** The ordering \leq_{DL} on A is called the *degree-lexicographic ordering*. Identify $(a, b) \in A$ with the monomial $X^a Y^b$. First, order monomials with respect to their degrees. For two monomials of the same degree, apply lexicographic ordering. For example, $XY^3 \leq_{DL} Y^5$ and $XY^3 \leq_{DL} X^2 Y^2$.
21. Generalize the degree-lexicographic ordering on \mathbb{N}^n for any fixed $n \geq 3$.
22. Consider the following relation ρ on the set \mathbb{Q}^+ of all positive rational numbers. Take $a/b, c/d \in \mathbb{Q}^+$ with $\gcd(a, b) = \gcd(c, d) = 1$. Call $(a/b) \rho (c/d)$ if and only if either (i) $a + b < c + d$ or (ii) $a + b = c + d$ and $a \leq c$. Prove that ρ is a total order.
23. Let A be the set of all functions $\mathbb{N} \rightarrow \mathbb{N}$. For $f, g \in A$, define $f \leq g$ if and only if $f(n) \leq g(n)$ for all $n \in \mathbb{N}$. prove that \leq is a partial order on A . Is \leq also a total order?
24. Let A be the set of all functions $\mathbb{N}_0 \rightarrow \mathbb{R}^+$.
- Define a relation Θ on A as $f \Theta g$ if and only if $f = \Theta(g)$. Prove that Θ is an equivalence relation.
 - Define a relation O on A as $f O g$ if and only if $f = O(g)$. Argue that O is not a partial order.
- Define a relation O on A/Θ as $[f] O [g]$ if and only if $f = O(g)$.
- Establish that the relation O is well-defined.
 - Prove that O is a partial order on A/Θ .
 - Prove or disprove: O is a total order on A/Θ .
 - Prove or disprove: A/Θ is a lattice under O .
25. Let k be a fixed positive integer. Define a relation \leq on $A = \mathbb{Z}^k$ as: $(a_1, a_2, \dots, a_k) \leq (b_1, b_2, \dots, b_k)$ if and only if $a_i \leq b_i$ for all $i = 1, 2, \dots, k$. Prove that A is a lattice under this relation.
26. Let A be a poset under the relation ρ . Prove or disprove:
- If ρ is a total order, then A is a lattice.
 - If A is a lattice, then ρ is a total order.
27. Let A be a poset. We call A a *meet-semilattice* (resp. *join-semilattice*) if $\text{glb}(a, b)$ (resp. $\text{lub}(a, b)$) exists for all $a, b \in A$. A is a lattice if and only if it is both a meet-semilattice and a join-semilattice. Give examples of:
- A meet-semilattice which is not a lattice.
 - A join-semilattice which is not a lattice.