CS21201 Discrete Structures

Tutorial 6

Sets, Relations, and Functions

1. Let $A, B, C \in \mathscr{U}$ are three arbitrary sets such that, $A \cup B = A \cup C$ and $A \cap B = A \cap C$. Prove that, $B = C$.

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

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 a 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 the equivalence classes $\mathbb{N}/\rho$.

Solution For all prime numbers, $p_1, p_2, \ldots, p_k, \ldots$, we have, $[p_k] = \{p_k^i \mid i \geqslant 1\}$

For all composite numbers, $q = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, we have, $[p_1 p_2 \cdots p_k] = \{q \mid p_i > 1,\ e_i > 0 \textit{ where } 1 \leqslant i \leqslant k\}$

(c) A non-zero integer is called *square-free* if it is not divisible by the square of a prime number. Prove that, each equivalence class in $\mathbb{N}/\rho$ contains a unique square-free integer, and that these unique square-free integers are different in distinct equivalence classes.

Solution Let $a \in \mathbb{N}$ have the prime factorization $a = p_1^{e_1} \cdots p_t^{e_t}$ with $t \geqslant 0$, pairwise distinct primes $p_1, \cdots, p_t$ and each $e_i > 0$. But, then a is related to the square-free integer $p_1 \cdots p_t$. No other square-free integer can have the same prime divisors as $p_1 \cdots p_t$. Thus, $[a]$ contains a unique square-free integer. Also if $[a] \neq [b]$, we have $[a] \cap [b] = \phi$ (ρ is an equivalence relation and so the equivalence classes partition $\mathbb{N}$), that is, the square-free integers in $[a]$ and $[b]$ are distinct.

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 (or itself 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 $\mathbb{R}/\rho$ is of the form, $[x] = \left\{x + r \mid r \in \mathbb{Q}\right\}$

(b) Equivalence classes $[y]$ of $\mathbb{R}/\sigma$ is of the form, $[y] = \left\{y + s \mid s \in \mathbb{Z}\right\}$

4. [*Genesis of rational numbers*] Define a relation ρ on $A = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ 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] If $(a, b)\ \rho\ (c, d)$ iff $ad = bc$, and $(c, d)\ \rho\ (e, f)$ iff $cf = de$, then we get, $(a, b)\ \rho\ (e, f)$, since $ad = bc \ \Rightarrow\ adf = bcf \ \Rightarrow\ adf = bde \ \Rightarrow\ af = be$ (as $d \neq 0$).

Equivalence classes of A/ρ are of the form, $[(a, b)] = \left[\frac{a}{b}\right] = \left\{\frac{na}{nb} \mid n \in \mathbb{N}\right\}$ and denotes the set $\mathbb{Q}$ of rationals.

5. For a function $f : A \to B$, define a function $\mathscr{F} : \mathscr{P}(A) \to \mathscr{P}(B)$ as $\mathscr{F}(S) = f(S)$ for all $S \subseteq A$, where $\mathscr{P}(A)$ and $\mathscr{P}(B)$ denote the power sets of A and B, respectively. Prove the following.

(a) $\mathscr{F}$ is injective if and only if f is injective.

Solution Note that $f(S) = \bigcup_{s \in S} f(s) \subseteq B$, where $S \subseteq A$.

[$\Leftarrow$] If f is injective, then we know that $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$, $(a_1, a_2 \in A)$. So, for $S_1, S_2 \subseteq A$, since we have $f(S_1) = \bigcup_{a_1 \in S_1} f(a_1)$ and $f(S_2) = \bigcup_{a_2 \in S_2} f(a_2)$, we have, $f(S_1) = f(S_2) \Rightarrow S_1 = S_2$. For $S_1, S_2 \in \mathscr{P}(S)$ and $S_1, S_2 \subseteq A$, we can say, $\mathscr{F}(S_1) = \mathscr{F}(S_2) \Rightarrow f(S_1) = f(S_2) \Rightarrow S_1 = S_2$. This concludes that $\mathscr{F}$ is injective.

[$\Rightarrow$] If $\mathscr{F}$ is injective, then for $S_1, S_2 \in \mathscr{P}(S)$ and $S_1, S_2 \subseteq A$, we can say, $\mathscr{F}(S_1) = \mathscr{F}(S_2) \Rightarrow S_1 = S_2$. Since $\mathscr{F}(S) = f(S)$ for all $S \subseteq A$, we can say, $f(S_1) = f(S_2) \Rightarrow S_1 = S_2$. Therefore, for $s_1 \in S_1$ and $s_2 \in S_2$, we have $f(s_1) = f(s_2) \Rightarrow s_1 = s_2$. This concludes that f is injective.

(b) $\mathscr{F}$ is surjective if and only if f is surjective.

Solution [$\Leftarrow$] If f is surjective, then we know that for all $b \in B$, there exists $a \in A$, such that $f(a) = b$. Therefore, for all $S_2 \subseteq B$, there exists $S_1 \subseteq A$, such that $f(S_1) = S_2$. It follows that for all $S_2 \in \mathscr{P}(B)$, there exists $S_1 \in \mathscr{P}(A)$, such that $\mathscr{F}(S_1) = S_2$. This concludes that $\mathscr{F}$ is surjective.

[$\Rightarrow$] If $\mathscr{F}$ is surjective, then we know that for all $S_2 \in \mathscr{P}(B)$, there exists $S_1 \in \mathscr{P}(A)$, such that $\mathscr{F}(S_1) = S_2$. As $\mathscr{F}(S) = f(S)$ for all $S \subseteq A$, it implies that for all $S_2 \subseteq B$, there exists $S_1 \subseteq A$, such that $f(S_1) = S_2$. It follows that for all $b \in S_2$, there exists $a \in S_1$, such that $f(a) = b$. This concludes that f is surjective.

(c) $\mathscr{F}$ is bijective if and only if f is bijective.

Solution The above parts (a) and (b) together prove this.

6. Let $f : A \to B$ 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] Also, $a \ \rho \ a'$ implies $f(a) \ \sigma \ f(a')$, that is, $f(a') \ \sigma \ f(a)$ (since σ is symmetric), that is, $a' \ \rho \ a$.
[ρ is transitive] Finally, $a \ \rho \ a'$ and $a' \ \rho \ a''$ imply $f(a) \ \sigma \ f(a')$ 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 $\bar{f} : A/\rho \to B/\sigma$ as $[a]_\rho \mapsto [f(a)]_\sigma$. Prove that $\bar{f}$ is well-defined.

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

[The question of well-defined-ness arises here, because the value of the function is defined in terms of a representative of a class. Thus, we needed to show that irrespective of the choice of the representative, we get the same value for the function. The assignment $g : \mathbb{Z}_5 \to \mathbb{Z}_6$ taking $[a]_5 \mapsto [a]_6$ is not well-defined. For example, $[0]_5 = [5]_5$, but $[0]_6 \neq [5]_6$, that is, we get different values when we use different representatives of the same class in the argument.]

(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.

(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.

[Note that, 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. In this exercise, we plan to construct a well-ordering of $A = \mathbb{N} \times \mathbb{N}$.

(a) First define a relation ρ on A as $(a,b)\ \rho\ (c,d)$ if and only if $a \leqslant c$ or $b \leqslant d$. Prove or disprove: ρ is a well-ordering of A.

Solution No. Indeed, ρ is not at all a partial order, since it is not antisymmetric: we have both $(1,2)\ \rho\ (2,1)$ and $(2,1)\ \rho\ (1,2)$, but $(1,2) \neq (2,1)$.

(b) Next, define a relation σ on A as $(a,b)\ \sigma\ (c,d)$ if and only if $a \leqslant c$ and $b \leqslant d$. Prove or disprove: σ is a well-ordering of A.

Solution No. One can easily check that σ is a partial order on A. However, it is not a total order (and hence cannot be a well-ordering of A): the pairs $(1,2)$ and $(2,1)$ are, for example, not comparable.

(c) Finally, define a relation $\leqslant_L$ on A as $(a,b) \leqslant_L (c,d)$ if either (i) $a < c$ or (ii) $a = c$ and $b \leqslant d$. Prove that, $\leqslant_L$ is a partial order on A.

Solution By Condition (ii), $(a,b) \leqslant_L (a,b)$. Now suppose that $(a,b) \leqslant_L (c,d)$ and $(c,d) \leqslant_L (a,b)$. If $a < c$, we cannot have $(c,d) \leqslant_L (a,b)$. Similarly, if $c < a$, we cannot have $(a,b) \leqslant_L (c,d)$. So $a = c$. But then $b \leqslant d$ and $d \leqslant b$, that is, $b = d$. Finally, suppose that $(a,b) \leqslant_L (c,d)$ and $(c,d) \leqslant_L (e,f)$. Then $a \leqslant c$ and $c \leqslant e$. If $a < c$ or $c < e$, then $a < e$. On the other hand, if $a = c = e$, we must have $b \leqslant d$ and $d \leqslant f$. But then $b \leqslant f$.

(d) Prove that $\leqslant_L$ is a total order on A.

Solution Take any (a,b) and (c,d) in A. If $a < c$, then $(a,b) \leqslant_L (c,d)$. If $a > c$, then $(c,d) \leqslant_L (a,b)$. Finally, suppose that $a = c$. Since either $b \leqslant d$ or $d \leqslant b$, we have either $(a,b) \leqslant_L (c,d)$ or $(c,d) \leqslant_L (a,b)$.

(e) Is A well-ordered under $\leqslant_L$?

Solution Yes. Let S be a non-empty subset of A. Take $X = \{a \in \mathbb{N} \mid (a,b) \in A \text{ for some } b \in \mathbb{N}\}$. Since S is non-empty, X is non-empty too and contains a minimum element; call it x. For this x, let $Y = \{b \in \mathbb{N} \mid (x,b) \in S\}$. Since Y is a non-empty subset of $\mathbb{N}$, it contains a minimum element; call it y. It is now an easy check that (x,y) is a minimum element of S.

(f) Prove or disprove: An infinite subset of A may contain a maximum element.

Solution True. The infinite subset $\{(1,b) \mid b \in N\} \cup \{(2,1)\}$ of A contains the maximum element $(2,1)$.

Note: The ordering $\leqslant_L$ on $\mathbb{N} \times \mathbb{N}$ described in this exercise is called the lexicographic ordering, since this is how you sort two-letter words in a dictionary. One can readily generalize this ordering to $\mathbb{N}^n$ for any $n > 3$.

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

Solution Take $A = \mathbb{Q}$ under the standard $\leqslant$ 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, $glb(S)$ 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.

9. Let $\mathbb{C}$ denote the set of complex numbers and $\mathbb{Z}[i]$ the subset $\{a + ib \mid a,b \in \mathbb{Z}\}$ of $\mathbb{C}$. Elements of $\mathbb{Z}[i]$ are called *Gaussian integers*. For $z = x + iy \in \mathbb{C}$, we denote by $|z|$ the magnitude of z and by $\arg z$ the argument of z. Thus, $z = \sqrt{x^2 + y^2}$ and $\arg z = \tan^{-1} \frac{y}{x}$. We take $\arg z$ in the interval $[0, 2\pi)$.

Define a relation ρ on $\mathbb{C}$ as follows. Take $z_1, z_2 \in \mathbb{C}$. We say that $z_1 \ \rho \ z_2$ if and only if

either (i) $|z_1| < |z_2|$,
or (ii) $|z_1| = |z_2|$ and $\arg z_1 \leqslant \arg z_2$.

Also define a relation σ on $\mathbb{C}$ as $z_1 \ \sigma \ z_2$ if and only if $|z_1| = |z_2|$.

(a) Prove that ρ is a partial order on $\mathbb{C}$.

Solution Let $z, z_1, z_2, z_3 \in \mathbb{C}$. We have $|z| = |z|$ and $\arg z \leqslant \arg z$, that is, $z \ \rho \ z$, that is, ρ is reflexive.

Then suppose $z_1 \ \rho \ z_2$ and $z_2 \ \rho \ z_1$. If $|z_1| < |z_2|$, we cannot have $z_2 \ \rho \ z_1$. Analogously, if $|z_2| < |z_1|$, we cannot have $z_1 \ \rho \ z_2$. Therefore, $|z_1| = |z_2|$. In that case, $\arg z_1 \leqslant \arg z_2$ and $\arg z_2 \leqslant \arg z_1$, that is, $\arg z_1 = \arg z_2$. It follows that $z_1 = z_2$, that is, ρ is antisymmetric.

Finally, let $z_1 \ \rho \ z_2$ and $z_2 \ \rho \ z_3$. This means $|z_1| \leqslant |z_2| \leqslant |z_3|$. If $|z_1| < |z_2|$ or $|z_2| < |z_3|$, then $|z_1| < |z_3|$, that is, $z_1 \ \rho \ z_3$. If $|z_1| = |z_2| = |z_3|$, we have $\arg z_1 \leqslant \arg z_2 \leqslant \arg z_3$, that is, again $z_1 \ \rho \ z_3$. Thus, ρ is transitive.

(b) Prove that ρ is a well-ordering of $\mathbb{Z}[i]$.

Solution Let S be a non-empty subset of $\mathbb{Z}[i]$. Consider the set $X = \{|z|^2 \mid z \in S\}$. X, being a non-empty subset of $\mathbb{N}$, contains a minimum element; call it n. Let $Y = \{z \in S \mid |z|^2 = n\}$. Since the equation $x^2 + y^2 = n$ can have only finitely many solutions in integer values of x and y, the set Y is finite. It is also non-empty. Thus, Y contains a minimum element; call it z. It is clear that this z is the minimum element of S with respect to ρ.

(c) Prove that σ is an equivalence relation on $\mathbb{C}$.

Solution Let $z, z_1, z_2, z_3 \in \mathbb{C}$. Since $|z| = |z|$, we have $z \ \sigma \ z$, that is, σ is reflexive.

Also $z_1 \ \sigma \ z_2$ implies $|z_1| = |z_2|$, that is, $|z_2| = |z_1|$, that is, $z_2 \ \sigma \ z_1$, that is, σ is symmetric.

Finally, $z_1 \ \sigma \ z_2$ and $z_2 \ \sigma \ z_3$ imply $|z_1| = |z_2| = |z_3|$, that is, $z_1 \ \sigma \ z_3$, that is, σ is transitive too.

(d) What are the equivalence classes of σ? (Provide a geometric description.)

Solution Let $z = x + iy \in \mathbb{C}$ with $r = \sqrt{x^2 + y^2}$. Then $[z]_\sigma$ consists precisely of all complex numbers whose absolute values equal r, that is, $[z]_\sigma$ is the circle of radius r centered at the origin.

10. Let $k \in \mathbb{N}$, $S = \{1, 2, \ldots, k\}$, and $A = \mathscr{P}(S) \setminus \{\phi\}$, where $\mathscr{P}(S)$ denotes the power set of S, and ϕ denotes the empty set. In other words, the set A comprises all non-empty subsets of $\{1, 2, \ldots, k\}$. 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, each equivalence class of ρ has a one-to-one correspondence with an element 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.

11. 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. In particular, every finite lattice is complete.

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

Since $S \neq \emptyset$, we have $n \geqslant 1$. For $n = 1,2$, the assertion about the existence of $lub(S)$ is obvious. So take $n \geqslant 3$, and assume that every $(n-1)$- and $(n-2)$-element subset of A has a least upper bound. Take $S = \{a_1, a_2, \ldots, a_n\} \subseteq A$. Since A is a lattice, $b = lub(a_{n-1}, a_n)$ exists. Let $T = \{a_1, a_2, \ldots, a_{n-2}, b\}$. 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 $i = 1,2,\ldots,n$. In particular, $a_{n-1} \preceq u$ and $a_n \preceq u$. Since $b = lub(a_{n-1}, a_n)$, we have $b \preceq u$, that is, $u \in U_T$. Conversely, if $u \in U_T$, then $a_i \preceq u$ for all $i = 1,2,\ldots,n-2$, 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 $lub(T)$. Since $U_S = U_T$, the same conclusions apply to S as well. It therefore follows that $lub(S) = lub(T)$.

(**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

12. Let $f : A \to B$ 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 $T \subseteq B$.

13. Let $f : A \to B$ and $g : B \to C$ be functions.

(a) Prove that if the function $g \circ f : A \to C$ 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.

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

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

15. A function $f : \mathbb{R} \to \mathbb{R}$ is called *monotonic increasing* if $f(a) \leqslant f(b)$ whenever $a \leqslant b$. 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 $\mathbb{R} \to \mathbb{R}$ need not be strictly increasing or strictly decreasing.
(c) Prove that a continuous injective function $\mathbb{R} \to \mathbb{R}$ is either strictly increasing or strictly decreasing.

16. Let A be the set of all functions $\mathbb{R} \to \mathbb{R}$. Define relations ρ, σ, τ on A as follows: (i) $f\ \rho\ g$ if and only if $f(a) \leqslant g(a)$ for all $a \in \mathbb{R}$; (ii) $f\ \sigma\ g$ if and only if $f(0) \leqslant g(0)$; (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).

17. 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.

18. 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 $\min(U) \leqslant \min(V)$. 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.

19. Let $f : A \to B$ 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 $\bar{f} : A/\rho \to B/\sigma$ given by $\bar{f}([a]_\rho) = [f(a)]_\sigma$ is not necessarily a function.

20. Let m, n be positive integers. Prove that the assignment $f : \mathbb{Z}_m \to \mathbb{Z}_n$ taking $[a]_m \mapsto [a]_n$ is well-defined if and only if m is an integral multiple of n.

*** 21.** [*Genesis of real numbers*] An infinite sequence $a_1, a_2, a_3, \ldots$ of rational numbers is called a *Cauchy sequence* if given any real $\varepsilon > 0$ there exists an $N \in \mathbb{N}$ such that $|a_m - a_n| < \varepsilon$ for all $m, n \geqslant N$. Let C denote the set of all Cauchy sequences of rational numbers.

(a) Prove that any Cauchy sequence converges, that is, has a limit.
(b) Establish that the limit of a Cauchy sequence may be irrational.
(c) Define a relation ρ on C as $S \,\rho\, T$ if and only if $\lim S = \lim T$. Prove that ρ is an equivalence relation.
(d) Convince yourself that C/ρ is essentially the set $\mathbb{R}$ of real numbers. This process of the generation of $\mathbb{R}$ from $\mathbb{Q}$ is called *completion*. Another method of defining $\mathbb{R}$ uses *Dedekind cuts*.

22. Let ρ be a total order on A. We call ρ a *well-ordering* of A if every non-empty subset of A contains a least element. Which of the following sets is/are well-ordered under the standard $\leqslant$ relation: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{R}$?

23. 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. Prove that this dictionary order (called *lexicographic ordering*) is a total ordering. Is it also a well-ordering?

24. Define a relation $\leqslant_{DL}$ on $A = \mathbb{N} \times \mathbb{N}$ as follows. Take $(a,b), (c,d) \in A$ and call $(a,b) \leqslant_{DL} (c,d)$ if either (i) $a + b < c + d$, or (ii) $a + b = c + d$ and $a \leqslant c$.

(a) Prove that $\leqslant_{DL}$ is a partial order on A.
(b) Prove that $\leqslant_{DL}$ is a total order on A.
(c) Is A well-ordered by $\leqslant_{DL}$?
(d) Prove or disprove: An infinite subset of A may contain a maximum element.

Note: The ordering $\leqslant_{DL}$ 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, $XY^3 \leqslant_{DL} Y^5$ and $XY^3 \leqslant_{DL} X^2Y^2$.

25. Generalize the degree-lexicographic ordering on $\mathbb{N}^n$ for any fixed $n \geqslant 3$.

26. 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 $a \leqslant c$. Prove that ρ is a total order. Prove that $\mathbb{Q}^+$ is well-ordered by ρ.

27. Construct a well-ordering of $\mathbb{Q}$.

28. Let A be the set of all functions $\mathbb{N} \to \mathbb{N}$. For $f, g \in A$, define $f \leqslant g$ if and only if $f(n) \leqslant g(n)$ for all $n \in \mathbb{N}$. prove that $\leqslant$ is a partial order on A. Is $\leqslant$ also a total order?

29. Let A be the set of all functions $\mathbb{N}_0 \to \mathbb{R}^+$.

- **(a)** Define a relation Θ on A as $f \,\Theta\, g$ if and only if $f = \Theta(g)$. Prove that Θ is an equivalence relation.
- **(b)** Define a relation O on A as $f \,\mathrm{O}\, g$ if and only if $f = \mathrm{O}(g)$. Argue that O is not a partial order.

Define a relation O on A/Θ as $[f] \;\mathrm{O}\; [g]$ if and only if $f = \mathrm{O}(g)$.

- **(c)** Establish that the relation O is well-defined.
- **(d)** Prove that O is a partial order on A/Θ.
- **(e)** Prove or disprove: O is a total order on A/Θ.
- **(f)** Prove or disprove: A/Θ is a lattice under O.

30. Let k be a fixed positive integer. Define a relation $\leqslant$ on $A = \mathbb{Z}^k$ as: $(a_1, a_2, \ldots, a_k) \leqslant (b_1, b_2, \ldots, b_k)$ if and only if $a_i \leqslant b_i$ for all $i = 1, 2, \ldots, k$. Prove that A is a lattice under this relation.

31. Let A be a poset under the relation ρ. Prove or disprove:

- **(a)** If ρ is a total order, then A is a lattice.
- **(b)** If A is a lattice, then ρ is a total order.

32. Let A be a poset. We call A a *meet-semilattice* (resp. *join-semilattice*) if $\mathrm{glb}(a, b)$ (resp. $\mathrm{lub}(a, b)$) 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)** A meet-semilattice which is not a lattice.
- **(b)** A join-semilattice which is not a lattice.