Relations and Functions Notes

Jason Sass

July 17, 2023

Relations

Definition 1. (binary) relation

A **relation** is a set of ordered pairs.

Definition 2. domain and range of a relation

Let R be a relation.

The **domain of** R, denoted $domR$, is the set $\{a : (\exists b)((a, b) \in R\}$.

The **range of** R, denoted $rngR$, is the set $\{b : (\exists a)((a, b) \in R\}$.

The field of R, denoted $fldR$, is the set $domR \cup rngR$.

Let R be a relation.

Then $domR = \{a : (\exists b)((a, b) \in R\}$ and $rngR = \{b : (\exists a)((a, b) \in R\}$ and $fldR = domR \cup rngR$.

Since $domR = \{a : (\exists b)((a, b) \in R\}$, then the domain of R is the set of elements that are the first elements of ordered pairs in R.

Since $rngR = \{b : (\exists a)((a, b) \in R\}$, then the range of R is the set of elements that are the second elements of ordered pairs in R.

Definition 3. relation between sets

A relation R is a relation between set A and set B iff $A = domR$ and $B = rngR$.

A relation R is a relation on A iff $A = fldR$.

Therefore, a relation is between its domain and its range and on its field.

Definition 4. domain and range of a relation

Let R be a relation from set A to set B.

The **domain of** R is the set $\{a \in A : (\exists b \in B)((a, b) \in R)\}$.

The **range of** R is the set $\{b \in B : (\exists a \in A)((a, b) \in R)\}$.

Let R be a relation from set A to set B.

Then $R \subset A \times B$, so R is a set of ordered pairs (a, b) such that $a \in A$ and $b \in B$.

Let $domR$ be the domain of R.

Then $domR = \{a \in A : (\exists b \in B)((a, b) \in R)\}$, so $domR \subset A$.

Therefore the domain of R is a subset of A and the domain of R is the set of elements of A that are the first elements of ordered pairs in R.

Let $rngR$ be the range of R.

Then $rngR = \{b \in B : (\exists a \in A)((a,b) \in R)\}$, so $rngR \subset B$.

Therefore the range of R is a subset of B and the range of R is the set of elements of B that are the second elements of ordered pairs in R.

Let $a \in domR$.

Then $a \in A$ and there exists $b \in B$ such that $(a,b) \in R$.

Since $b \in B$ and $a \in A$ and $(a,b) \in R$, then $b \in rngR$.

Thus, $b \in rngR$ and $(a,b) \in R$.

Therefore, for each $a \in domR$, there exists $b \in rngR$ such that $(a,b) \in R$.

Hence, if R is a relation, then for each $a \in domR$, there exists $b \in rngR$ such that $(a,b) \in R$.

A relation between sets defines an association between sets.

Definition 5. binary relation between sets

Let A, B be sets.

A **relation from** A **to** B is a subset of $A \times B$.

Therefore R is a **relation** from A to B iff $R \subset A \times B$.

If $A = B$, then R is a **relation on** A.

Therefore, R is a relation on A iff $R \subset A \times A$.

Let R be a relation from a set A to a set B.

Then $R \subset A \times B$, so R is a set of ordered pairs (a,b) such that $a \in A$ and $b \in B$.

Let $(a,b) \in R$.

Since $R \subset A \times B$, then $(a,b) \in A \times B$, so $a \in A$ and $b \in B$.

We say that R relates a to b.

aRb denotes that a is R related to b.

Therefore, aRb iff $(a,b) \in R$.

Hence, $a \not R b$ iff $(a,b) \notin R$.

Thus, $R = \{(a,b) \in A \times B : aRb\}$.

Let R be a relation on a set S.

Then $R \subset S \times S$, so R is a set of ordered pairs (a,b) such that $a \in S$ and $b \in S$.

Let $(a,b) \in R$.

Since $R \subset S \times S$, then $(a,b) \in S \times S$, so $a, b \in S$.

We say that R relates a to b.

aRb denotes that a is R related to b.

Therefore, aRb iff $(a,b) \in R$.

Hence, $a \not R b$ iff $(a,b) \notin R$.

Thus, $R = \{(a,b) \in S \times S : aRb\}$.

(S,R) denotes a relation R defined over a set S.

Example 6. Let $A = \{1,2,3\}$ and $B = \{w,x,y,z\}$.

Let $R_1 = \{(1,x),(2,y),(3,z)\}$.

Then $R_1 \subset A \times B$, so R_1 is a relation from A to B.
Let $R_2 = \{(2, w), (2, x), (2, y), (2, z)\}$.
Then $R_2 = \{(2, b) : b \in B\}$ and R_2 is a relation from A to B.
Let $R_3 = \{(1, z), (2, z), (3, z)\}$.
Then $R_3 = \{(a, z) : a \in A\}$ and R_3 is a relation from A to B.
Let $R_4 = \{(x, 1), (x, 3)\}$.
Then $R_4 \subset B \times A$, so R_4 is a relation from B to A.

Example 7. empty relation $\emptyset$
Let A, B be sets.
Since the empty set is a subset of every set, then in particular, $\emptyset \subset A \times B$.
Therefore, the empty set is a relation from A to B called the **empty relation**.
Let E be the empty relation.
Then $E = \{(a, b) \in A \times B : aEb\} = \emptyset$.
Let $a \in A, b \in B$.
Then aEb iff $(a, b) \in E$.
Since $E = \emptyset$, then $(a, b) \in E$ is false.
Hence, aEb is false.
Therefore, for every $a \in A, b \in B$, aEb is false.

Example 8. total relation $A \times B$
Let A, B be sets.
Since every set is a subset of itself, then $A \times B \subset A \times B$.
Therefore, $A \times B$ is a relation from A to B called the **total relation**.
Let T be the total relation.
Then $T = \{(a, b) \in A \times B : aTb\} = A \times B = \{(a, b) : a \in A, b \in B\}$.
Let $a \in A, b \in B$.
Then aTb iff $(a, b) \in T$.
Since $a \in A$ and $b \in B$, then $(a, b) \in A \times B$.
Since $A \times B = T$, then $(a, b) \in T$.
Therefore, aTb.
Hence, for every $a \in A, b \in B$, aTb is true.

Let S be a set.
Then $S \times S$ is the total relation on S.

Example 9. equals relation defined on a set
On any set $a = b$ iff a and b denote the same mathematical object.
Let S be a set.
The set $I_S = \{(x, x) \in S \times S : x \in S\} = \{(x, x) : x \in S\} = \{(a, b) \in S \times S : a = b\}$ is called the **identity relation on** X, also known as the **equality relation**.

Example 10. less than relation on $\mathbb{R}$
The relation $<$ on $\mathbb{R}$ is a subset of $\mathbb{R} \times \mathbb{R}$ consisting of all ordered pairs (a, b) of real numbers such that $a < b$.
Thus, $<$ is $\{(a, b) \in \mathbb{R} \times \mathbb{R} : (\exists c > 0)(a + c = b)\}$.

Example 11. subset relation on the power set of a set

Let S be a set.

Let $\mathscr{P}$ be the power set of S.

The subset relation $\subset$ on $\mathscr{P}$ is a subset of $\mathscr{P} \times \mathscr{P}$ consisting of all ordered pairs (X, Y) such that $X \subset Y$.

Therefore, the subset relation $\subset$ is the set $\{(X, Y) \in \mathscr{P} \times \mathscr{P} : X \subset Y\}$.

Definition 12. properties of relations

Let R be a relation defined over a set S.

Then $R \subset S \times S$.

1. R is **reflexive** iff $(\forall a \in S)(aRa)$.
2. R is **symmetric** iff $(\forall a, b \in S)(aRb \to bRa)$.
3. R is **antisymmetric** iff $(\forall a, b \in S)[(aRb \wedge bRa) \to (a = b)]$.
4. R is **transitive** iff $(\forall a, b, c \in S)[(aRb \wedge bRc) \to aRc]$.

Example 13. Let $<$ be the less than relation on $\mathbb{R}$.

Since $6 < 6$ is false, then $<$ is not reflexive.

Since $8 < 9$ is true, but $9 < 8$ is false, then $<$ is not symmetric.

Since $x < y$ and $y < z$ implies $x < z$ for all $x, y, z \in \mathbb{R}$, then $<$ is transitive.

Let $a, b \in \mathbb{R}$ such that $a < b$ and $b < a$.

By trichotomy of $\mathbb{R}$, the statement $a < b$ and $b < a$ is false.

Therefore, the conditional $a < b$ and $b < a$ implies $a = b$ is vacuously true.

Hence, $<$ is antisymmetric.

Definition 14. inverse relation

Let R be a relation from set A to set B.

The **inverse relation,** R **inverse,** is the set $R^{-1} = \{(b, a) : (a, b) \in R\}$.

Let R be a relation from set A to set B.

Then $R \subset A \times B$ and $(b, a) \in R^{-1}$ iff $(a, b) \in R$.

Let $(y, x) \in R^{-1}$.

Then $(x, y) \in R$.

Since $R \subset A \times B$, then $(x, y) \in A \times B$.

Hence, $x \in A$ and $y \in B$, so $(y, x) \in B \times A$.

Since $(y, x) \in R^{-1}$ implies $(y, x) \in B \times A$, then $R^{-1} \subset B \times A$.

Therefore, if $R \subset A \times B$, then $R^{-1} \subset B \times A$.

Proposition 15. *Let R be a nonempty relation from set A to set B. Then*

1. *dom R^{-1} = range R.*
2. *range R^{-1} = dom R.*
3. $(R^{-1})^{-1} = R$.

Proposition 16. *Let R be a nonempty relation on a set S. Then*

1. *R is reflexive iff $I_S \subset R$.*
2. *R is symmetric iff $R = R^{-1}$.*

Ex. inverse of $\leq$ is $\geq$

Definition 17. composition of relations
Let R and S be relations.
The **composition of** R **and** S is the relation $S \circ R = \{(a, b) : (\exists c)((a, c) \in R \wedge (c, b) \in S)\}$.

Since the composition of two relations is a set of ordered pairs, then the composition of two relations is a relation.

Example 18. Let $r = \{(1, 3), (2, 7), (3, 10), (4, 17), (5, 20)\}$ and $s = \{(4, 3), (6, 5), (10, 20)\}$.
Then $s \circ r = \{(3, 20)\}$ and $r \circ s = \{(4, 10), (6, 20)\}$.
Since $s \circ r \neq r \circ s$, then composition of relations is not commutative.

Proposition 19. *Let r and s be relations. Then*
$r \circ s \subset dom\ s \times rng\ r$.

$\circ$ is a binary operation on $\{X : X \subset S \times S\}$ = the set of all binary relations on set S.

Composition of relations is associative.
Therefore, $(R \circ S) \circ T = R \circ (S \circ T)$.

Let R be a relation.
Then $R \circ R = R^2$, $R \circ R \circ R = R^3$, etc.

Equivalence Relations

Each element of a set is distinct.
So, if we want to treat certain elements of a set as being the 'same', then we must define a relation that defines when two elements are equivalent.

Definition 20. equivalence relation on a set
Let $\sim$ be a relation defined over a set S.
Then $\sim$ is an **equivalence relation over** S iff
1. $\sim$ **is reflexive:** aRa
2. $\sim$ **is symmetric:** $aRb \Rightarrow bRa$
3. $\sim$ **is transitive:** aRb and $bRc \Rightarrow aRc$

Example 21. Equality relation on a set is an equivalence relation
Let S be a set.
Let $I_S = \{(s, s) : s \in S\} = \{(a, b) \in S \times S : a = b\}$ be the equality relation on S.
Then the equality relation, also known as the identity relation, is an equivalence relation on S.

Example 22. total relation on a set is an equivalence relation
Let S be a set.
Let $S \times S = \{(a, b) : a, b \in S\}$ be the total relation on S.
Then $S \times S$ is an equivalence relation on S.

Example 23. cardinality relation on the power set of a finite set
Let S be a finite set.
Let $\mathscr{P}$ be the power set of S.
Let $R = \{(A, B) \in \mathscr{P} \times \mathscr{P} : A$ and B contain the same number of elements $\} = \{(A, B) \in \mathscr{P} \times \mathscr{P} : |A| = |B|\}$.
Then R is an equivalence relation on $\mathscr{P}$.

Definition 24. Let R be a relation on a set S.
Define for each $x \in S$ the set $[x] = \{y \in S : (y, x) \in R\}$.
The set $[x]$ is the set of all elements of S that are related to x.

Let R be a relation over a set S.
Let $x \in S$.
Then $[x] \subset S$ and $[x] = \{y \in S : yRx\}$.

Example 25. Let $S = \{1, 2, 3, 4, 5\}$.
Let $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 3), (3, 2), (1, 3), (3, 1), (4, 5), (5, 4)\}$.
Since $R \subset S \times S$, then R is a relation on S.
Since $(5, 5) \notin R$, then R is not reflexive.
Hence, R is not an equivalence relation.
$[1] = \{y \in S : y \sim 1\} = \{1, 3\}$
$[2] = \{y \in S : y \sim 2\} = \{1, 2, 3\}$
$[3] = \{y \in S : y \sim 3\} = \{1, 2, 3\}$
$[4] = \{y \in S : y \sim 4\} = \{4, 5\}$
$[5] = \{y \in S : y \sim 5\} = \{4\}$.

Example 26. Let $S = \{1, 2, 3, 4, 5\}$.
Let $R = \{(2, 2), (3, 3), (4, 4), (5, 5), (3, 4), (4, 3), (3, 5), (5, 3), (4, 5), (5, 4)\}$.
Since $R \subset S \times S$, then R is a relation on S.
Observe that R is symmetric and transitive.
However, $(1, 1) \notin R$, so R is not reflexive.
Therefore, R is not an equivalence relation.
$[1] = \{y \in S : y \sim 1\} = \emptyset$
$[2] = \{y \in S : y \sim 2\} = \{2\}$
$[3] = \{y \in S : y \sim 3\} = \{3, 4, 5\}$
$[4] = \{y \in S : y \sim 4\} = \{3, 4, 5\}$
$[5] = \{y \in S : y \sim 5\} = \{3, 4, 5\}$.

Definition 27. equivalence class and quotient set of an equivalence relation
Let R be an equivalence relation over a set S.
The **equivalence class of** $x \in S$ is the set $[x] = \{y \in S : y \sim x\}$.
The set of all equivalence classes of R, called the **quotient set of** S **by** R, is $\frac{S}{R} = \{[x] : x \in S\}$.

Let $\sim$ be an equivalence relation defined over a set S.
Let $x \in S$.

The equivalence class of x is the set of all elements of S that are equivalent to x.

Therefore, $[x] = \{y \in S : y \sim x\}$ and $[x] \subset S$.

Let $s \in [x]$.

Then $s \in S$ and $s \sim x$.

The set of all equivalence classes of $\sim$ is $\frac{S}{\sim} = \{[x] : x \in S\}$.

Since each $[x]$ is a subset of S, then $\frac{S}{\sim}$ is a subset of the powerset of S.

Example 28. Let $S = \{1, 2, 3, 4, 5\}$.

Let $R = \{(1,1),(2,2),(3,3),(4,4),(5,5),(2,5),(5,2),(3,5),(5,3),(2,3),(3,2)\}$.

Since $R \subset S \times S$, then R is a relation on S.

Since R is reflexive, symmetric, and transitive, then R is an equivalence relation on S.

The equivalence classes are:

$[1] = \{x \in S : x \sim 1\} = \{1\}$

$[2] = \{x \in S : x \sim 2\} = \{2, 3, 5\} = [3] = [5]$

$[4] = \{x \in S : x \sim 4\} = \{4\}$.

The collection of equivalence classes of R is

$\frac{S}{R} = \{[x] : x \in S\} = \{\{1\}, \{2, 3, 5\}, \{4\}\}$.

Theorem 29. *Let $\sim$ be an equivalence relation on a set S. Then*

1. $a \in [a]$ for all $a \in S$.

2. $a \in [b]$ iff $a \sim b$ for all $a, b \in S$.

3. $[a] = [b]$ iff $a \sim b$ for all $a, b \in S$.

4. for all $a, b \in S$, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

5. $\cup([a] : a \in S) = S$.

Corollary 30. *Let $\sim$ be an equivalence relation on set S.*

Then each element of S is an element of exactly one equivalence class.

Definition 31. partition of a set

A **partition of a set** S is a collection of disjoint non-empty subsets of S that have S as their union.

Let S be a set.

A collection P of subsets of S is a **partition of** S iff

1. $(\forall T \in P)(T \neq \emptyset)$.
2. for all $T_1, T_2 \in P$, either $T_1 = T_2$ or $T_1 \cap T_2 = \emptyset$.
3. $(\forall x \in S)(\exists T \in P)(x \in T)$.

Let S be a set.

Let P be a collection of subsets of S such that

1. $(\forall T \in P)(T \neq \emptyset)$.
2. for all $T_1, T_2 \in P$, either $T_1 = T_2$ or $T_1 \cap T_2 = \emptyset$.
3. $(\forall x \in S)(\exists T \in P)(x \in T)$.

Then P is a partition of S.

Each element T of the partition P is called a **cell** of the partition.

Let $T \in P$.

Then $T \subset S$ and T is a cell of the partition P.
Condition 1 implies each cell is nonempty.
Condition 2 implies any two cells are either identical or disjoint.
Observe that

$$(\forall T_1, T_2 \in P)(T_1 = T_2 \vee T_1 \cap T_2 = \emptyset) \quad \Leftrightarrow \quad (\forall T_1, T_2 \in P)(T_1 \neq T_2 \rightarrow T_1 \cap T_2 = \emptyset).$$

Therefore any two distinct cells are disjoint.
Condition 3 implies every element of S is in at least one cell.
Let $x \in S$.
Then there exists $T \in P$ such that $x \in T$.
Since $\cup(T : T \in P) = \{x \in S : (\exists T \in P)(x \in T)\}$, then $x \in \cup(T : T \in P)$.
Thus, $x \in S$ implies $x \in \cup(T : T \in P)$, so $S \subset \cup(T : T \in P)$.
Since $\cup(T : T \in P) = \{x \in S : (\exists T \in P)(x \in T)\}$, then $\cup(T : T \in P) \subset S$.
Since $\cup(T : T \in P) \subset S$ and $S \subset \cup(T : T \in P)$, then $\cup(T : T \in P) = S$.
Therefore the union of all elements of P is S.
Hence, the union of all cells of P is S.

Example 32. Let $T_1 = \{2k \in \mathbb{Z} : k \in \mathbb{Z}\}$ be the set of all even integers.
Let $T_2 = \{2k + 1 \in \mathbb{Z} : k \in \mathbb{Z}\}$ be the set of all odd integers.
Let $P = \{T_1, T_2\}$.
Then P is a 2 celled partition of $\mathbb{Z}$.

Example 33. Let T_1 be the set of all rational numbers.
Let T_2 be the set of all irrational numbers.
Let $P = \{T_1, T_2\}$.
Then P is a 2 celled partition of $\mathbb{R}$.

Example 34. Let $P = \{(0, \infty), \{0\}, (-\infty, 0)\}$.
Then P consists of the positive real numbers, the set containing zero, and the negative real numbers.
Therefore P is a 3 celled partition of $\mathbb{R}$.

Example 35. Let S be a set.
Let $P = \{\{x\} : x \in S\}$ be a collection of singleton cells.
If S is infinite, then P is a partition of S with infinitely many cells.

Example 36. Let $P = \{\{0\}, \{-1, 1\}, \{-2, 2\}, ...\}$.
Then P is a partition of $\mathbb{Z}$ with infinitely many cells.

Example 37. Let $S = \{1, 2, 3, 4, 5\}$.
Then $\{\{1, 5\}, \{3, 4\}, \{2\}\}$ and $\{\{1, 2, 3, 5\}, \{4\}\}$ are partitions of S.

Theorem 38. ***Any partition of a set yields a corresponding equivalence relation***
Let S be a nonempty set.
Let P be a partition of S.
Define a relation $\sim$ on S by $a \sim b$ iff there exists a cell $T \in P$ such that $a \in T$ and $b \in T$ for all $a, b \in S$.
Then $\sim$ is an equivalence relation on S.

The equivalence relation $\sim$ is induced by the partition P of a set S in a canonical way.

We denote it by the symbol $\frac{S}{P}$ and call it the **equivalence relation determined by the partition** P.

Example 39. Let $S = \{1, 2, 3, 4, 5\}$.

Let $P = \{\{2\}, \{1, 3, 4\}, \{5\}\}$.

Since P is a partition of S, the equivalence relation $\frac{S}{P}$ is the set consisting of the ordered pairs $(2, 2), (1, 1), (3, 3), (4, 4), (1, 3), (3, 1), (1, 4), (4, 1), (3, 4), (4, 3), (5, 5)$.

Theorem 40. ***Any equivalence relation on a set yields a corresponding partition***

Let $\sim$ be an equivalence relation on a nonempty set S.

Then the collection $\frac{S}{\sim} = \{[x] : x \in S\}$ of equivalence classes induced by $\sim$ is a partition of S.

Let $\frac{S}{\sim}$ be the collection of all equivalence classes of an equivalence relation $\sim$ defined over a set S.

Then the quotient set $\frac{S}{\sim} = \{[x] : x \in S\}$ is a partition of S.

Therefore, an equivalence relation over a set S partitions S into a collection of equivalence classes.

Example 41. Let $S = \{1, 2, 3, 4, 5\}$.

Let R be a relation consisting of

$(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 3), (3, 1), (1, 4), (4, 1), (3, 4), (4, 3), (2, 5), (5, 2)$.

Then R is an equivalence relation on S and the quotient set $\frac{S}{R} = \{[x] : x \in S\} = \{\{1, 3, 4\}, \{2, 5\}\}$ is a partition of S.

The equivalence relation induced by the partition $\frac{S}{R}$ is the set $\frac{S}{\frac{S}{R}}$ consisting of

$(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 3), (3, 1), (1, 4), (4, 1), (3, 4), (4, 3), (2, 5), (5, 2)$.

Therefore, $\frac{S}{\frac{S}{R}} = R$, the original relation.

Example 42. Let $S = \{1, 2, 3, 4, 5\}$.

Let $P = \{\{1\}, \{2, 3\}, \{4\}, \{5\}\}$.

Then P is a partition of S.

The equivalence relation $\frac{S}{P}$ induced by the partition P is the set consisting of the ordered pairs $(1, 1), (2, 2), (2, 3), (3, 2), (3, 3), (4, 4), (5, 5)$.

The set of equivalence classes of $\frac{S}{P}$ is the set $\frac{S}{\frac{S}{P}} = \{[x] : x \in S\} = \{\{1\}, \{2, 3\}, \{4\}, \{5\}\}$.

Therefore, $\frac{S}{\frac{S}{P}} = P$, the original partition.

Theorem 43. *If R is an equivalence relation on a set S, then $\frac{S}{\frac{S}{R}} = R$.*

If P is a partition of a set S, then $\frac{S}{\frac{S}{P}} = P$.

Proposition 44. *If E_1 and E_2 are equivalence relations on a set S, then $E_1 \cap E_2$ is an equivalence relation on S.*

Theorem 45. *Let $\sim$ be an equivalence relation over a set S.*

Let $\frac{S}{\sim} = \{[a] : a \in S\}$.

Let $f : S \to \frac{S}{\sim}$ be a binary relation from S to $\frac{S}{\sim}$ defined by $f(a) = [a]$ for all $a \in S$.

Then f is a surjective function.

Definition 46. Natural Projection of S onto $\frac{S}{\sim}$

Let $\sim$ be an equivalence relation defined over a set S.

Let $\frac{S}{\sim}$ be the set of all equivalence classes of $\sim$.

Define a binary relation $\eta : S \to \frac{S}{\sim}$ by $\eta(a) = [a]$ for all $a \in S$.

Then η is a surjective function called the **natural projection of S onto $\frac{S}{\sim}$**.

Theorem 47. *Let $\sim$ be an equivalence relation over a set S.*

Let f be the natural projection of S onto $\frac{S}{\sim}$.

Then $x_1 \sim x_2$ iff $f(x_1) = f(x_2)$ for all $x_1, x_2 \in S$.

Proposition 48. *Let $f : A \to B$ be a function.*

Let $\sim$ be a relation defined on A by $x_1 \sim x_2$ iff $f(x_1) = f(x_2)$ for all $x_1, x_2 \in A$.

Then $\sim$ is an equivalence relation on A.

Therefore every function $f : A \to B$ determines an equivalence relation $\sim$ on the set A, called the kernel of f.

The collection of all equivalence classes of A under $\sim$ is $\frac{A}{\ker f} = \{[a] : a \in A\}$.

Hence, every equivalence relation on A comes from some function $f : A \to B$.

Definition 49. kernel of a function

Let $f : A \to B$ be a function.

The **kernel of** f is the equivalence relation defined on A by $a \sim b$ iff $f(a) = f(b)$ for all $a, b \in A$.

The kernel of f is denoted $\ker f$.

Therefore $\ker f = \{(a, b) \in A \times A : a \sim b\} = \{(a, b) \in A \times A : f(a) = f(b)\}$.

Theorem 50. *Let $f : A \to B$ be a function.*

Let $\ker f$ be the kernel of f.

Then there is a bijection from $\frac{A}{\ker f}$ to $f(A)$.

Moreover, $f^{-1}(b)$ is an equivalence class of A under $\ker f$ for every $b \in f(A)$.

Let $g : \frac{A}{\ker f} \mapsto f(A)$ be a binary relation from $\frac{A}{\ker f}$ to $f(A)$ defined by $g([x]) = f(x)$ for all $[x] \in \frac{A}{\ker f}$.

Then $g : \frac{A}{\ker f} \mapsto f(A)$ is a bijective function.

Partial Orders

Since a set is an unordered collection of objects, if we want to order the elements of a set, we must define a relation that defines how to order elements of a set.

Therefore we define the partial order concept on a set.

Definition 51. partial ordering on a set

Let S be a set.

Let $\leq$ be a relation defined over S.

Then $\leq$ is a **partial ordering over** S iff

1. $\leq$ is reflexive
2. $\leq$ is antisymmetric
3. $\leq$ is transitive

We say that the set S is **partially ordered under** $\leq$ and $\leq$ is a partial order over S.

A nonempty set with a partial ordering is called a **poset** or **partially ordered set**.

Let $\leq$ be a partial ordering over a nonempty set S.

Then $(S, \leq)$ is a poset and S is partially ordered under $\leq$.

Let $a, b \in S$.

Then $a \leq b$ means 'a precedes b'.

Then $a \nleq b$ means 'a does not precede b'.

Example 52. The relation $<$ on $\mathbb{R}$ is antisymmetric and transitive.

However, $<$ is not reflexive since for example, $3.5 < 3.5$ is false.

Therefore, $<$ is not a partial ordering over $\mathbb{R}$.

Example 53. The relation $\leq$ on $\mathbb{R}$ is reflexive, antisymmetric, and transitive, so $\leq$ is a partial ordering over $\mathbb{R}$.

Therefore, $(\mathbb{R}, \leq)$ is a poset.

Example 54. The power set of a set is ordered by inclusion.

Let S be a set.

Then $(2^S, \subset)$ is a poset.

Let 2^S be the power set of a set S.

Let R be the subset relation over 2^S.

Then $R = \{(M, N) \in 2^S \times 2^S : M \subset N\}$.

Since $\subset$ is reflexive, antisymmetric, and transitive, then R is a partial order over 2^S, so $(2^S, \subset)$ is a poset.

Therefore the subset relation defines a partial ordering on the power set of S, so

1. R is reflexive: $A \subset A$ for any subset A of S.
2. R is antisymmetric: if $A \subset B$ and $B \subset A$, then $A = B$ for any subsets A, B of S.
3. R is transitive: if $A \subset B$ and $B \subset C$, then $A \subset C$ for any subsets A, B, C of S.

Hasse Diagram = graph of a partial ordering

1. Draw directed graph of R.
2. Remove all loops at each vertex that has reflexivity.
3. Remove all edges due to transitivity.

4. Make each initial vertex of an edge below its terminal vertex.

5. Remove each arrow on each edge since all edges point up toward their terminal vertex.

a) Bottom most element(s) = minimal element(s)

b) Top most element(s) = maximal element(s)

Example 55. Let $S = \{1, 2, 3\}$.

Then $|2^S| = 2^{|S|} = 2^3 = 8$, so there are 8 subsets of S.

Thus, 2^S consists of the following:

$\emptyset$

$\{1\}, \{2\}, \{3\}$

$\{1, 2\}, \{1, 3\}, \{2, 3\}$

$\{1, 2, 3\}$.

Let R be a relation on 2^S such that $(A, B) \in R$ iff $A \subset B$ for all $A, B \in 2^S$.

Then $R = \{(A, B) \in 2^S \times 2^S : A \subset B\}$, so R is the subset relation on 2^S.

The elements of R are:

$(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{3\}), (\emptyset, \{1, 2\}), (\emptyset, \{1, 3\}), (\emptyset, \{2, 3\}), (\emptyset, \{1, 2, 3\})$

$(\{1\}, \{1\}), (\{1\}, \{1, 2\}), (\{1\}, \{1, 3\}), (\{1\}, \{1, 2, 3\})$

$(\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{2\}, \{2, 3\}), (\{2\}, \{1, 2, 3\})$

$(\{3\}, \{3\}), (\{3\}, \{1, 3\}), (\{3\}, \{2, 3\}), (\{3\}, \{1, 2, 3\})$

$(\{1, 2\}, \{1, 2\}), (\{1, 2\}, \{1, 2, 3\})$

$(\{1, 3\}, \{1, 3\}), (\{1, 3\}, \{1, 2, 3\})$

$(\{2, 3\}, \{2, 3\}), (\{2, 3\}, \{1, 2, 3\})$

$(\{1, 2, 3\}, \{1, 2, 3\})$

Since $(2^S, \subset)$ is a poset for any set S, then in particular $(2^S, \subset)$ is a poset.

We draw the Hasse(lattice) diagram of 2^S which shows the ordering of the elements of 2^S under the subset relation R.

Example 56. The divides relation defined on the set of all nonnegative integers is a partial order.

Since $\mathbb{Z}^+ \cup \{0\}$ is the set of all nonnegative integers and $|$ is the divides relation, then $(\mathbb{Z}^+ \cup \{0\}, |)$ is a poset.

Example 57. Let V be the set of all positive divisors of 24.

Then $V = \{d \in \mathbb{Z}^+ : d|24\} = \{1, 2, 3, 4, 6, 8, 12, 24\}$.

Let E be a binary relation on V such that $(a, b) \in E$ iff $a|b$ for all $a, b \in V$.

Then $E = \{(a, b) \in V \times V : a|b\}$, so E is the divides relation on V.

The elements of E are:

$(1, 1), (1, 2), (1, 3), (1, 4), (1, 6), (1, 8), (1, 12), (1, 24)$

$(2, 2), (2, 4), (2, 6), (2, 8), (2, 12), (2, 24)$

$(3, 3), (3, 6), (3, 12), (3, 24)$

$(4, 4), (4, 8), (4, 12), (4, 24)$

$(6, 6), (6, 12), (6, 24)$

$(8, 8), (8, 24)$

$(12, 12), (12, 24)$

$(24, 24)$.

Since $(\mathbb{Z}^+ \cup \{0\}, |)$ is a poset and $V \subset \mathbb{Z}^+ \cup \{0\}$, then $(V, |)$ is a poset.

Therefore, V is partially ordered under the divides relation E.

We draw the Hasse(lattice) diagram of V which shows the ordering of the elements of V under the divides relation E.

The Hasse diagram is the directed graph $G = (V, E)$.

Example 58. Let $S = \{1, 2, 3, 4, 6, 8, 12, 24\}$.

Under the relation $\leq$, the set S is ordered linearly, so $(S, \leq)$ is a poset.

Thus, $(S, \leq)$ is a poset and $(S, |)$ is a different poset

Thus, a set may have different partial orders defined on it.

Definition 59. bounded poset

Let $(P, \leq)$ be a partially ordered set.

Let $S \subset P$.

An element $u \in P$ is an **upper bound for** S iff $(\forall x \in S)(x \leq u)$.

The set S is **bounded above in** P iff S has an upper bound in P.

Therefore, S is bounded above in P iff $(\exists u \in P)(\forall x \in S)(x \leq u)$.

An element $l \in P$ is a **lower bound for** S iff $(\forall x \in S)(l \leq x)$.

The set S is **bounded below in** P iff S has a lower bound in P.

Therefore, S is bounded below in P iff $(\exists l \in P)(\forall x \in S)(l \leq x)$.

The set S is **bounded in** P iff S is bounded above in P and bounded below in P.

The set S is **unbounded in** P iff S is not bounded.

Example 60. an upper bound of a set need not be unique

Consider the poset $(\mathbb{R}, \leq)$.

Let $S = \{-3.1, 1.5, 2\} \subset \mathbb{R}$.

Then 2.5 is an upper bound for S since $-3.1 \leq 2.5$ and $1.5 \leq 2.5$ and $2 \leq 2.5$.

Similarly, 2 is an upper bound for S since $-3.1 \leq 2$ and $1.5 \leq 2$ and $2 \leq 2$.

Thus, an upper bound of a set need not be unique.

Example 61. The interval $(1, \infty)$ is unbounded above in $\mathbb{R}$ and bounded below in $\mathbb{R}$.

Example 62. The interval $(0, 1)$ is bounded in $\mathbb{R}$.

Example 63. The interval $(0, 1]$ is bounded below in $\mathbb{R}$, but not bounded below in $\mathbb{R}^+$.

Example 64. In the poset $(\mathbb{R}, \leq)$, 0 is a lower bound for the intervals $[0, 1]$ and $(0, 1]$.

Proposition 65. *Any element of a partially ordered set is an upper and lower bound of $\emptyset$.*

Let $(S, \leq)$ be a poset.

Let $x \in S$.

Then x is an upper and lower bound of $\emptyset$.

Definition 66. greatest element of a poset (maximum)
Let $(P, \leq)$ be a partially ordered set.
Let $S \subset P$.
Then M is a **greatest element of** S iff
1. $M \in S$.
2. $(\forall x \in S)(x \leq M)$. M is an upper bound of S.

Definition 67. least element of a poset (minimum)
Let $(P, \leq)$ be a partially ordered set.
Let $S \subset P$.
Then m is a **least element of** S iff
1. $m \in S$.
2. $(\forall x \in S)(m \leq x)$. m is a lower bound of S.

Example 68. In the poset $(\mathbb{R}, \leq)$, 7 is a greatest element of the interval $(-\infty, 7]$ since $7 \in (-\infty, 7]$ and $x \leq 7$ for every $x \in (-\infty, 7]$.

Example 69. poset bounded above need not have a greatest element
In the poset $(\mathbb{R}, \leq)$, the intervals $[0, 1]$ and $(0, 1)$ are bounded above and $[0, 1]$ has a greatest element, but $(0, 1)$ does not have a greatest element.

Example 70. Let $S = \{1 - \frac{1}{n} : n \in \mathbb{N}\}$.
In the poset $(\mathbb{R}, \leq)$, 1 is an upper bound for S, but S has no greatest element.

Theorem 71. ***uniqueness of maximum of a poset***
Let $(P, \leq)$ be a poset.
Let $S \subset P$.
The greatest element of S, if it exists, is unique.

Theorem 72. ***uniqueness of minimum of a poset***
Let $(P, \leq)$ be a poset.
Let $S \subset P$.
The least element of S, if it exists, is unique.

Example 73. Let S be a set.
In the poset $(2^S, \subset)$ S is the greatest element and $\emptyset$ is the least element.

Example 74. In the poset $(\mathbb{Z}^+ \cup \{0\}, |)$ 0 is the greatest element and 1 is the least element.

Definition 75. least upper bound of a poset (supremum)
Let $(P, \leq)$ be a partially ordered set.
Let $S \subset P$.
Then $U \in P$ is a **least upper bound of** S iff U is the least element of the set of all upper bounds of S in P.
Therefore $U \in P$ is a **least upper bound of** S iff
1. $(\forall x \in S)(x \leq U)$. ($U$ is an upper bound for S)
2. for each $u \in P$, if $x \leq u$ for all $x \in S$, then $U \leq u$. (U is less than or equal to any upper bound of S)

Theorem 76. ***uniqueness of least upper bound of a poset***

Let $(P, \leq)$ be a poset.

Let $S \subset P$.

The least upper bound of S, if it exists, is unique.

Let $(P, \leq)$ be a poset and $S \subset P$.

Let B be the set of all upper bounds of S in P.

Then $B = \{u \in P : u \text{ is an upper bound of } S\}$ and $B \subset P$.

The **least upper bound (lub) of** S is called the **supremum** and is denoted $\sup S$.

Therefore, $\sup S$ is the least element of B.

Example 77. In the poset $(\mathbb{R}, \leq)$ let $S = (0, 1)$ and $T = [0, 1]$.

Then $\sup(S) = 1 = \sup(T)$ and $\sup(S) \notin S$ and $\sup(T) \in T$ and there is no greatest element in S and 1 is the greatest element of T.

Definition 78. greatest lower bound of a poset (infimum)

Let $(P, \leq)$ be a partially ordered set.

Let $S \subset P$.

Then $L \in P$ is a **greatest lower bound of** S iff L is the greatest element of the set of all lower bounds of S in P.

Therefore $L \in P$ is a **greatest lower bound of** S iff

1. $(\forall x \in S)(L \leq x)$. ($L$ is a lower bound for S)

2. for each $l \in P$, if $l \leq x$ for all $x \in S$, then $l \leq L$. (any lower bound of S is less than or equal to L)

Theorem 79. ***uniqueness of greatest lower bound of a poset***

Let $(P, \leq)$ be a poset.

Let $S \subset P$.

The greatest lower bound of S in P, if it exists, is unique.

Let $(P, \leq)$ be a poset and $S \subset P$.

Let B be the set of all lower bounds of S in P.

Then $B = \{l \in P : l \text{ is a lower bound of } S\}$ and $B \subset P$.

The **greatest lower bound (glb) of** S is called the **infimum** and is denoted $\inf S$.

Therefore, $\inf S$ is the greatest element of B.

Theorem 80. ***sufficient conditions for existence of supremum and infimum of a poset***

Let S be a subset of a partially ordered set P.

1. If $\max S$ exists, then $\sup S = \max S$.

2. If $\min S$ exists, then $\inf S = \min S$.

If $\max S$ does not exist, then $\sup S$, if it exists, is not in S.

We prove by contrapositive.

Suppose $\sup S$ exists and $\sup S \in S$.

Since $\sup S$ is an upper bound of S and $\sup S \in S$, then $\sup S = \max S$.

Therefore, $\max S$ exists.
If $\min S$ does not exist, then $\inf S$, if it exists, is not in S.
We prove by contrapositive.
Suppose $\inf S$ exists and $\inf S \in S$.
Since $\inf S$ is a lower bound of S and $\inf S \in S$, then $\inf S = \min S$.
Therefore, $\min S$ exists.

Definition 81. comparable
Let $(S, \leq)$ be a poset.
Let $a, b \in S$.
Then a **and** b **are comparable** iff either $a \leq b$ or $b \leq a$.

Observe that $\neg(a \leq b \vee b \leq a) \Leftrightarrow (a \not\leq b \wedge b \not\leq a)$.
Therefore a and b are not comparable iff $a \not\leq b \wedge b \not\leq a$.

Example 82. Consider the poset $(\mathbb{Z}^+ \cup \{0\}, |)$.
Since $6|18$ is true, then the disjunction $6|18 \vee 18|6$ is true.
Therefore, 6 and 18 are comparable under the divides relation.
Since $2|5$ is false and $5|2$ is false, then the disjunction $2|5 \vee 5|2$ is false.
Therefore, 2 and 5 are not comparable under the divides relation.
Hence, the poset $(\mathbb{Z}^+ \cup \{0\}, |)$ is not a total order.

Example 83. Consider the poset $(2^{\mathbb{N}}, \subset)$.
Since $\{1,2\} \subset \{1,2,4\}$, then the disjunction $\{1,2\} \subset \{1,2,4\} \vee \{1,2,4\} \subset \{1,2\}$ is true.
Therefore, $\{1,2\}$ and $\{1,2,4\}$ are comparable under the subset relation.
Since $\{1,2\} \not\subset \{2,3\}$ and $\{2,3\} \not\subset \{1,2\}$, then the disjunction $\{1,2\} \subset \{2,3\} \vee \{2,3\} \subset \{1,2\}$ is false.
Therefore, $\{1,2\}$ and $\{2,3\}$ are not comparable under the subset relation.
Hence, the poset $(2^{\mathbb{N}}, \subset)$ is not a total order.

Definition 84. total ordering on a set
A total order is a partial order in which any two elements are comparable.
Let $(S, \leq)$ be a partially ordered set.
Then $\leq$ is a **total order over** S iff $(\forall a, b \in S)(a \leq b \vee b \leq a)$.
A set with a total order is called a **linearly ordered set or chain**.

Let $(S, \leq)$ be a linearly ordered set.
Then $\leq$ is a total order over the set S.
Hence, any two elements of S are comparable, so $(\forall a, b \in S)(a \leq b \vee b \leq a)$.
Therefore, every element of S is related to every other element.

The Hasse diagram of a linear order is linear.

Example 85. The poset $(\mathbb{R}, \leq)$ is a total order.

Example 86. Let $S \subset \mathbb{R}$.
Then $(S, \leq)$ is a total order.
Therefore, any subset of $\mathbb{R}$ is linearly ordered under the relation $\leq$.

Example 87. Since $\mathbb{N} \subset \mathbb{R}$, then $(\mathbb{N}, \leq)$ is a linear order.

Example 88. Let S be any set.
The poset $(2^S, \subset)$ is not a total order.

Examples:
a. the lexicographic order of words in a dictionary
b. Let $S = \{(m, n) : m, n \in \mathbb{N}\}$.
Define $(m, n) \leq (m', n')$ iff either $m < m'$, or $m = m' \wedge m \leq n'$.
Then S is a linearly ordered set.

Definition 89. well ordering of a linearly ordered set
Let $(S, \leq)$ be a totally ordered set.
Then S is **well ordered** iff every nonempty subset of S has a least element.

Definition 90. meet/join
Let $(S, \leq)$ be a poset.
Let $x, y \in S$.
The element $lub\{x, y\}$, if it exists, is denoted by $x \vee y$ and is called the **join of x and y**.
The element $glb\{x, y\}$, if it exists, is denoted by $x \wedge y$ and is called the **meet of x and y**.

Definition 91. Maximal element of a Poset
A **maximal element** of a poset is an element $m \in S$ that is not smaller than any other element.
Therefore, m is **maximal** iff $\neg(\exists s \in S)(s > m)$.
There may exist multiple maximal elements in a poset yet no greatest element exists.

Definition 92. Minimal element of a Poset
An **minimal element** of a poset is an element $m \in S$ that is not larger than any other element.
Therefore, m is **minimal** iff $\neg(\exists s \in S)(s < m)$.
There may exist multiple minimal elements in a poset yet no least element exists.
There may exist some element that is both minimal and maximal.

Not every pair of elements in a poset need be related-it is possible neither element precedes the other.

Representation of relations

Representation of a relation.
A. Relation R can be viewed as a mapping $R : S \to S$.
B. Relation R can be represented as a directed graph $G = \langle V, E \rangle$ where
V = vertex set = $\{v \in S : v \text{ is a vertex}\}$
E = edge set = $\{(a, b) \in R : (a, b) \text{ is an edge}\}$

Let S be a finite set with $|S| = n, n \in \mathbb{Z}^+$.
Then there are 2^{n^2} different binary relations on S.
A. Graph Representation of a relation from A to B.
Let A, B be sets.
Let R be a binary relation from A to B.
R can be represented as a directed graph $G = \langle V, E \rangle$ such that
$V =$ vertex set $= A \cup B$
$E =$ edge set $= \{$ edge from a to b $: (\forall a \in A)(\forall b \in B)(aRb)\}$.
C. Matrix Representation
Let A, B be finite sets.
Relation $R : A \mapsto B$ can be viewed as a matrix M_R with $|A|$ rows and $|B|$ columns.
if $A_i R B_j$ then assign 1 to $M[i][j]$ for i^{th} element of A and j^{th} element of B.
if $A_i \not R B_j$ then assign 0 to $M[i][j]$ for i^{th} element of A and j^{th} element of B.

$S \circ R =$ R*S where
$R =$ matrix representation of relation R and
$S =$ matrix representation of relation S and
to multiply = use logical AND
to add = use logical OR

Functions

Definition 93. function
A **function** is a relation f such that if $(a, b) \in f$ and $(a, b') \in f$, then $b = b'$.

Let f be a function.
Then f is a relation such that if $(a, b) \in f$ and $(a, b') \in f$, then $b = b'$.
Since f is a relation, then f is a set of ordered pairs.
Let $dom f$ be the domain of f and let $rng f$ be the range of f.
Then $dom f = \{a : (\exists b)(a, b) \in f\} = \{a : (\exists b)(f(a) = b)\} = \{a : f(a) \text{ exists}\}$.
Then $rng f = \{b : (\exists a)(a, b) \in f\} = \{b : (\exists a)(f(a) = b)\} = \{f(a) : a \text{ exists}\} = \{f(a) : a \in dom f\}$.
Since f is a relation, then for each $a \in dom f$, there exists $b \in rng f$ such that $(a, b) \in f$.

Let $a \in dom f$.
Then there exists at least one $b \in rng f$ such that $(a, b) \in f$.
Suppose there exists b' such that $(a, b') \in f$.
Since f is a function and $(a, b) \in f$ and $(a, b') \in f$, then $b = b'$.
Hence, there exists at most one $b \in rng f$ such that $(a, b) \in f$.
Thus, there exists exactly one $b \in rng f$ such that $(a, b) \in f$, so there is a unique $b \in rng f$ such that $(a, b) \in f$.

Define the statement 'b is the value of the function f at a' by $f(a) = b$ iff $(a, b) \in f$.

Then there is a unique $b \in rngf$ such that $f(a) = b$.

Thus, if $a \in domf$, then there is a unique $b \in rngf$ such that $f(a) = b$.

Therefore, if f is a function, then for each $a \in domf$, there is a unique $b \in rngf$ such that $f(a) = b$.

A relation specified by a listing of its ordered pairs is a function iff no two distinct ordered pairs in the list have the same first element.

A function may be described by specifying its domain and a rule of correspondence $y = f(x)$ for all x in the domain of f.

If $x \in domf$, we say that y is the value of the function f at x and write $y = f(x)$.

A relation f is not a function iff there exists $(a, b) \in f$ and $(a, b') \in f$ and $b \neq b'$.

Example 94. Let $f_1 = \{(2, 3), (3, 5), (4, 7), (5, 9)\}$.

Let $f_2 = \{(1, 1), (1, -1), (4, 7), (5, 9)\}$.

Then f_1 and f_2 are relations and f_1 is a function.

Since $(1, 1) \in f_2$ and $(1, -1) \in f_2$, but $1 \neq -1$, then f_2 is not a function.

Example 95. identity function

Let S be a set.

The **identity function on** S, denoted I_S, is defined by the rule $I_S(x) = x$ for all $x \in S$.

Example 96. constant function

Let S be a set.

Let $k \in S$.

The **constant function defined on** S, denoted $C : S \to S$, is defined by the rule $C(x) = k$ for all $x \in S$.

Proposition 97. ***A function value is unique.***

Let f be a function.

Let $a, b \in domf$.

If $a = b$, then $f(a) = f(b)$.

Let f be a function.

If $a \in domf$, then $f(a)$ is unique.

The negation of $(\forall a, b \in domf)(a = b \to f(a) = f(b))$ is $(\exists a, b \in domf)(a = b \wedge f(a) \neq f(b))$.

Hence, a relation f is not a function iff there exists $a, b \in domf$ such that $a = b$ and $f(a) \neq f(b)$.

Let $f : A \to B$ be a relation.

To prove f is a function we must show f is **well defined**.

Thus we must prove:

1. **Existence** $(\forall a \in A)(\exists b \in B)[f(a) = b]$.
2. **Uniqueness** $(\forall a, b \in A)(a = b \to f(a) = f(b))$.

If either condition is not satisfied by f, then f is not a function.

Let f and g be functions.

Then $f = g$ iff f and g are the same set of ordered pairs.

Theorem 98. ***equality of functions***

Let f and g be functions.

Let $domf$ be the domain of f.

Let $domg$ be the domain of g.

Then $f = g$ iff

1. $domf = domg$.

2. $f(x) = g(x)$ for all $x \in domf \cap domg$.

Let f and g be functions.

Then $f = g$ iff

1. domain of f equals the domain of g.
2. $f(x) = g(x)$ for all x in the common domain.

Definition 99. map from set A to set B

A **map from set A to set B**, denoted $f : A \to B$, consists of a function f such that $domf = A$ and $rngf \subset B$.

The set B is called the **codomain** of f.

Let $f : A \to B$ be a map from set A to set B.

We say that "$f : A \to B$ is a map from A to B" or "f is a function that maps A to B".

Let $f : A \to B$ be a map from set A to set B.

Then f is a function such that $domf = A$ and $rngf \subset B$.

Since f is a function, then for each $a \in domf$, there is a unique $b \in rngf$ such that $f(a) = b$.

Thus, for each $a \in A$, there is a unique $b \in rngf$ such that $f(a) = b$.

Since $rngf \subset B$, then for each $a \in A$, there is a unique $b \in B$ such that $f(a) = b$.

Thus, if $f : A \to B$ is a map from set A to set B, then f is a function and A is the domain of f and B is the codomain of f and $rngf \subset B$ and for each $a \in A$, there is a unique $b \in B$ such that $f(a) = b$.

A map $f : A \to B$ assigns to each $a \in A$ a unique $b \in B$.

Definition 100. identity map on a set

Let S be a set.

Let $I_S : S \to S$ be a map defined by $I_S(x) = x$ for all $x \in S$.

We call I_S the **identity map on** S.

Therefore, I_S maps each element of S onto itself.
Since I_S is a bijective function on S, then I_S is a permutation map on S.

Example 101. constant map
Let $k \in \mathbb{R}$.
Let $C : \mathbb{R} \to \mathbb{R}$ be the map given by $C(x) = k$ for all $x \in \mathbb{R}$.
The map is called a constant map and the range of C, the set $\{k\}$, is a subset of the codomain $\mathbb{R}$.

Example 102. distinct maps can specify the same function
Let $f_1 : \mathbb{R} \to \mathbb{R}$ be defined by $f_1(x) = x^2$.
Let $f_2 : \mathbb{R} \to [0, \infty)$ be defined by $f_2(x) = x^2$.
Observe that f_1 and f_2 specify the same function, the square function.
Since $\mathbb{R} \neq [0, \infty)$, then f_1 and f_2 are distinct maps.

Definition 103. equal maps
The maps $f : A \to B$ and $g : C \to D$ are **equal** iff $f = g$ and $B = D$.

Proposition 104. *equality of maps*
The maps $f : A \to B$ and $g : C \to D$ are equal iff
1. $A = C$.
2. $B = D$.
3. $f(x) = g(x)$ for all $x \in A$.

Maps $f : A \to B$ and $g : C \to D$ are equal iff
1. $A = C$ (same domain)
2. $B = D$ (same codomain)
3. $f(x) = g(x)$ for all x in the common domain A.

Definition 105. restriction of a map
Let $f : A \to B$ be a map.
Let $S \subset A$.
Let $f|_S : S \to B$ be defined by $f|_S(x) = f(x)$ for all $x \in S$.
We call $f|_S$ the **restriction of f to S**.

Proposition 106. *restriction of a map is a map*
Let $f : A \to B$ be a map.
Let $S \subset A$.
Let $f|_S : S \to B$ be defined by $f|_S(x) = f(x)$ for all $x \in S$.
Then $f|_S : S \to B$ is a map.

Example 107. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^2$.
Let $f|_{[0,\infty)}(x) = x^2$ for all $x \in [0, \infty)$.
Then the function $g : [0, \infty) \to \mathbb{R}$ defined by $g(x) = \sqrt{x}$ is the inverse of $f|_{[0,\infty)}$, the restriction of f to $[0, \infty)$.

Definition 108. inclusion map
Let $S \subset U$.
Let $i : S \to U$ be a map defined by $i(x) = x$ for all $x \in S$.
We call i the **inclusion map of S into U**.
Thus, i assigns to each element of S the same element, now in U.

Example 109. inclusion map is a restriction of the identity map

Let $I : S \to S$ be the identity map on a set S.

Then $I(x) = x$ for all $x \in S$.

Let $X \subset S$.

Let $i : X \to S$ defined by $i(x) = x$ for all $x \in X$ be the inclusion map.

Then the inclusion map $i : X \to S$ is the restriction $I|_X$ of the identity map to the set X.

If f and g are functions, then f and g are relations, so the composition of f and g is a relation.

Definition 110. composition of functions

Let f and g be functions.

The **composition of f and g** is the relation $g \circ f = \{(a, b) : (\exists c)((a, c) \in f \wedge (c, b) \in g\}$.

Theorem 111. ***Composition of functions is a function.***

Let f and g be functions. Then

1. $g \circ f$ is a function.

2. dom $g \circ f = \{x \in domf : f(x) \in domg\}$.

3. $(g \circ f)(x) = g(f(x))$ for all $x \in$ dom $g \circ f$.

Theorem 112. ***Function composition is associative.***

Let f, g, h be functions.

Then $(f \circ g) \circ h = f \circ (g \circ h)$.

Example 113. Function composition is not commutative.

Let $f = \{(1, 2), (2, 3), (3, 4), (4, 5), (5, 6), (6, 7)\}$.

Let $g = \{(2, 4), (3, 5), (4, 6), (5, 7), (7, 2)\}$.

Then f and g are functions, so $f \circ g$ and $g \circ f$ are functions.

Since $f \circ g = \{(2, 5), (3, 6), (4, 7), (7, 3)\}$ and $g \circ f = \{(1, 4), (2, 5), (3, 6), (4, 7), (6, 2)\}$, then $f \circ g \neq g \circ f$.

Proposition 114. ***Composition of maps***

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

Then $g \circ f : A \to C$ is a map and $(g \circ f)(x) = g(f(x))$ for all $x \in A$.

Proposition 115. *Let $f : A \to B$ be a map.*

Let I_A be the identity map on A and I_B be the identity map on B.

Then $f \circ I_A = I_B \circ f = f$.

An injective map preserves distinctness; an injective map maps distinct elements in the domain to distinct elements in the range.

Therefore, a map is injective iff no two distinct ordered pairs have the same second element.

Definition 116. injective map (one to one)
A map $f : A \to B$ is said to be **one to one**, or **injective**, iff the function f is a one to one function; that is, for every $a, b \in A$ if $f(a) = f(b)$, then $a = b$.
Such a map is said to be an **injection** of A into B.

Let $f : A \to B$ be a map.
Then f is injective iff
the function f is one to one iff
$(\forall a, b \in A)(f(a) = f(b) \to a = b)$ iff
$(\forall a, b \in A)(a \neq b \to f(a) \neq f(b))$.

Therefore, f is not injective iff
the function f is not one to one iff
$(\exists a, b \in A)(a \neq b \wedge f(a) = f(b))$.

Theorem 117. ***Left cancellation property of injective maps***
Let $f : X \to Y$ be a map.
Then f is injective iff for every set W and every map $g : W \to X$ and $h : W \to X$ such that $f \circ g = f \circ h$ we have $g = h$.

A surjective map is a map whose range equals its codomain.

Definition 118. surjective map (onto)
A map $f : A \to B$ is said to be **onto**, or a **function that maps** A **onto** B iff $rngf = B$.
We say that such a map is **surjective**, or a **surjection**.

Let $f : A \to B$ be a surjective map.
Then $f(A) = rngf = \{f(a) \in B : a \in A\} = B$.

Proposition 119. *A map $f : A \to B$ is surjective iff $(\forall b \in B)(\exists a \in A)(f(a) = b)$.*

Let $f : A \to B$ be a map.
Then f is surjective iff $(\forall b \in B)(\exists a \in A)[f(a) = b]$.
Therefore, f is not surjective iff $(\exists b \in B)(\forall a \in A)[f(a) \neq b]$.

Theorem 120. ***Right cancellation property of surjective maps***
Let X be a nonempty set.
Let $f : X \to Y$ be a map.
Then f is surjective iff for every set Z and every map $g : Y \to Z$ and $h : Y \to Z$ such that $g \circ f = h \circ f$ we have $g = h$.

Definition 121. bijective map (one to one correspondence)
Let $f : A \to B$ be a map.
Then f is **bijective** iff f is injective and surjective.
A **bijection** is a bijective function.

Let $f : A \to B$ be a map.
Then f is not bijective iff either f is not injective or f is not surjective.

Proposition 122. ***identity map is bijective.***
Let S be a set.
The identity map $I_S : S \to S$ on S is a bijection.

Theorem 123. *Let $f : A \to B$ and $g : B \to C$ be maps.*
1. If f and g are injective, then $g \circ f$ is injective.
A composition of injections is an injection.
2. If f and g are surjective, then $g \circ f$ is surjective.
A composition of surjections is a surjection.
3. If $g \circ f$ is injective, then f is injective.
4. If $g \circ f$ is surjective, then g is surjective.

Corollary 124. *Let $f : A \to B$ and $g : B \to C$ be maps.*
1. If f and g are bijective, then $g \circ f$ is bijective.
A composition of bijections is a bijection.
2. If $g \circ f$ is bijective, then f is injective and g is surjective.

Let f be a function.
Since f is a relation, then the inverse relation f^{-1} exists and is unique.

Definition 125. inverse of a function
Let f be a function.
The **inverse of** f is the inverse relation $f^{-1} = \{(b, a) : (a, b) \in f\}$.

Let f be a function.
Then f^{-1} is the inverse of f and $f^{-1} = \{(b, a) : (a, b) \in f\}$, so $(b, a) \in f^{-1}$ iff $(a, b) \in f$.
Therefore, $f^{-1}(b) = a$ iff $f(a) = b$ for all $a \in dom f$.
Since f is a relation, then $dom f^{-1} = rng f$ and $rng f^{-1} = dom f$ and $(f^{-1})^{-1} = f$.

Example 126. Let $f = \{(3, 5), (5, 8), (7, 11), (9, 14), (11, 17)\}$.
Then f is a function and the inverse of f is $f^{-1} = \{(5, 3), (8, 5), (11, 7), (14, 9), (17, 11)\}$.

Theorem 127. ***existence of inverse function***
Let f be a function.
Then the inverse relation f^{-1} is a function iff f is injective.

Definition 128. invertible map
A map $f : A \to B$ is said to be **invertible** iff there exists a map $g : B \to A$ such that g is an inverse of f.

Theorem 129. ***The inverse of an invertible map is unique.***
Let $f : A \to B$ be an invertible map.
Then the inverse map is unique.

Let $f : A \to B$ be an invertible map.
Then there exists a unique map $g : B \to A$ such that g is an inverse of f.
Since g is the unique inverse of f, we denote g by f^{-1}.
Thus, the inverse map of f is $f^{-1} : B \to A$.
Therefore, $f^{-1}(b) = a$ iff $f(a) = b$ for every $a \in A$ and $b \in B$.
Therefore, a map $f : A \to B$ is invertible iff the inverse map $f^{-1} : B \to A$ exists.

Theorem 130. *Let $f : A \to B$ and $g : B \to A$ be maps.*
Then g is an inverse of f iff
1. $g \circ f = I_A$
2. $f \circ g = I_B$.

Let $f : A \to B$ and $g : B \to A$ be maps such that g is an inverse of f.
Then $g \circ f : A \to A$ and $f \circ g : B \to B$ are maps and $g \circ f = I_A$ and $f \circ g = I_B$.
Since $g \circ f = I_A$, then $(\forall a \in A)[(g \circ f)(a) = a]$.
Since $f \circ g = I_B$, then $(\forall b \in B)[(f \circ g)(b) = b]$.

Corollary 131. *Let $f : A \to B$ be an invertible map. Then*
1. $f^{-1} \circ f = I_A$
2. $f \circ f^{-1} = I_B$.

Let $f : A \to B$ be an invertible map.
Then the inverse map $f^{-1} : B \to A$ exists, so $f^{-1} \circ f : A \to A$ and $f \circ f^{-1} : B \to B$ are maps and $f^{-1} \circ f = I_A$ and $f \circ f^{-1} = I_B$.
Since $f^{-1} \circ f = I_A$, then $(\forall a \in A)[(f^{-1} \circ f)(a) = a]$.
Since $f \circ f^{-1} = I_B$, then $(\forall b \in B)[(f \circ f^{-1})(b) = b]$.

Theorem 132. ***An invertible map is bijective.***
Let $f : A \to B$ be a map.
Then f is invertible iff f is bijective.

Example 133. The inverse of the identity map on a set is the identity map on the set.
Let I_S be the identity map on a set S.
Then $I_S^{-1} = I_S$.

Lemma 134. *Let $f : A \to B$ be a map.*
If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is a bijection.

Let $f : A \to B$ be a bijective map.
Since f is bijective, then f is invertible, so the inverse map $f^{-1} : B \to A$ exists.
Therefore,
1) $f^{-1} \circ f = I_A$.
2) $f \circ f^{-1} = I_B$.

Theorem 135. *Let $f : A \to B$ be a bijection. Then*
1. $(f^{-1})^{-1} : A \to B$ *is a bijection.*
2. $(f^{-1})^{-1} = f$.

Theorem 136. *Let $f : A \to B$ and $g : B \to C$ be bijections. Then*
1. $(g \circ f)^{-1} : C \to A$ *is a bijection.*
2. $f^{-1} \circ g^{-1} : C \to A$ *is a bijection.*
3. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Image and inverse image of functions

Definition 137. image of an element of a map

Let $f : A \to B$ be a map.
Let $(a, b) \in f$.
Then $a \in A$ and $b \in B$ and $f(a) = b$.
$f(a) = b$ means f maps a to b
b is the **image** of a under f.
a is the **preimage** of b under f.

Since f is a function, then
1) $(\forall a \in A)(\exists b \in B)[f(a) = b]$.
Every element in the domain has at least one image.
2) $(\forall a \in A)[f(a)$ is unique$]$.
The image of every element in the domain is unique.

Definition 138. preimage of an element in the codomain of a map

Let $f : A \to B$ be a map.
Let $b \in B$.
The **pre-image of** b is the set $f^{-1}(b) = \{a \in A : f(a) = b\}$.
Therefore $f^{-1}(b) \subset A$.

Proposition 139. *Let $f : A \to B$ be a map.*
1. *Then f is injective iff every $b \in B$ has at most one pre-image.*
2. *Then f is surjective iff every $b \in B$ has at least one pre-image.*
3. *Then f is bijective iff every $b \in B$ has exactly one pre-image.*

Definition 140. image of a subset of the domain of a map

Let $f : A \to B$ be a map.
Let $S \subset A$.
The **image of S under** f is the set $f(S) = \{f(x) : x \in S\}$.

Let $f : A \to B$ be a map.
Let $S \subset A$.
Suppose $f(x) \in f(S)$.
Then $x \in S$.
Since $S \subset A$, then $x \in A$.
Since $f : A \to B$ is a map, then $f(x) \in B$.
Hence, $f(S) \subset B$.
Therefore, the image of a subset of the domain of a map is a subset of the codomain of the map.

Let $b \in B$.
Then $b \in f(S)$ iff $b = f(x)$ for some $x \in S$.

Definition 141. inverse image of a subset of the codomain of a map
Let $f : A \to B$ be a map.
Let $T \subset B$.
The **inverse image of T under f** is the set $f^{-1}(T) = \{x \in A : f(x) \in T\}$.

Let $f : A \to B$ be a map.
Let $T \subset B$.
Since $f^{-1}(T) = \{x \in A : f(x) \in T\}$, then $f^{-1}(T) \subset A$.
Therefore, the inverse image of a subset of the codomain of a map is a subset of the domain of the map.

Let $x \in A$.
Then $x \in f^{-1}(T)$ iff $f(x) \in T$.

Proposition 142. *Let $f : A \to B$ be a map. Then*
1. $f(\emptyset) = \emptyset$.
The image of the empty set is the empty set.
2. $f^{-1}(\emptyset) = \emptyset$.
The inverse image of the empty set is the empty set.
3. $f(A) = rngf$.
The image of the domain of f is the range of f.
4. $f^{-1}(B) = A$.
The inverse image of the codomain of f is the domain of f.

Definition 143. image of a map(function)
Let $f : A \to B$ be a map.
The **image of** f is the set $f(A) = \{f(x) : x \in A\}$.

Proposition 144. *Let $f : X \to Y$ be a map.*
1. For every subset A and B of X, if $A \subset B$, then $f(A) \subset f(B)$.
2. $f(A \cup B) = f(A) \cup f(B)$ for every subset A and B of X.
The image of a union equals the union of the images.
3. $f(A \cap B) \subset f(A) \cap f(B)$ for every subset A and B of X.
The image of an intersection is a subset of the intersection of the images.
4. $f(A \cap B) = f(A) \cap f(B)$ for every subset A and B of X iff f is injective.

Proposition 145. *Let $f : X \to Y$ be a map.*
1. For every subset C and D of Y, if $C \subset D$, then $f^{-1}(C) \subset f^{-1}(D)$.
2. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$ for every subset C and D of Y.
The inverse image of a union equals the union of the inverse images.
3. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$ for every subset C and D of Y.
The inverse image of an intersection equals the intersection of the inverse images.

Proposition 146. ***inverse image of the image of a subset of the domain of a map***

Let $f : A \to B$ be a map. Then

1. $S \subset f^{-1}(f(S))$ for every subset S of A.

2. $f^{-1}(f(S)) = S$ for every subset S of A iff f is injective.

Proposition 147. ***image of the inverse image of a subset of the codomain of a map***

Let $f : A \to B$ be a map. Then

1. $f(f^{-1}(T)) \subset T$ for every subset T of B.

2. $f(f^{-1}(T)) = T$ for every subset T of B iff f is surjective.

Let A, B be finite sets, $|A| = m$ and $|B| = n$.

Let B^A = the set of all functions from A to B.

Then $B^A = \{f : A \to B | f \text{ is a function.}\}$.

Then $|B^A| = |B|^{|A|}$.

Thus, there are n^m different functions from A to B.

There are $P(n, m) = \frac{n!}{(n-m)!}$ different 1-1 functions from A to B.