Relations and Functions Theory

Jason Sass

July 16, 2023

Relations

Proposition 1. *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. *$(R^{-1})^{-1} = R$.*

Proof. We prove $domR^{-1} = rangeR$.

Since R is not empty, then there is at least one ordered pair in R.

Let x be an arbitrary object in the domain of discourse.

We prove dom R^{-1} = range R.

Observe that

$$\begin{aligned} x \in domR^{-1} &\Leftrightarrow x \in B \wedge (\exists y \in A)((x, y) \in R^{-1}) \\ &\Leftrightarrow x \in B \wedge (\exists y \in A)((y, x) \in R) \\ &\Leftrightarrow x \in rangeR. \end{aligned}$$

Therefore, $domR^{-1} = rangeR$. □

Proof. We prove range R^{-1} = dom R.

Observe that

$$\begin{aligned} x \in rangeR^{-1} &\Leftrightarrow x \in A \wedge (\exists y \in B)((y, x) \in R^{-1}) \\ &\Leftrightarrow x \in A \wedge (\exists y \in B)((x, y) \in R) \\ &\Leftrightarrow x \in domR. \end{aligned}$$

Therefore, range R^{-1} = dom R. □

Proof. We prove $(R^{-1})^{-1} = R$.

Let (a, b) be arbitrary.

Then

$$\begin{aligned} (a, b) \in (R^{-1})^{-1} &\Leftrightarrow (b, a) \in R^{-1} \\ &\Leftrightarrow (a, b) \in R. \end{aligned}$$

Therefore, $(R^{-1})^{-1} = R$. □

Proposition 2. *A relation R on a nonempty set S is reflexive iff $I_S \subset R$.*

Proof. Let S be a nonempty set.

Since S is not empty, then there is an element in S, so let a be an element of S.

Let R be a relation on S.

We must prove R is reflexive iff $I_S \subset R$.

We first prove if R is reflexive, then $I_S \subset R$.

Suppose R is reflexive.

Let $(a, a) \in I_S$ be arbitrary.

Since R is reflexive and $a \in S$, then $(a, a) \in R$.

Hence, $(a, a) \in I_S$ implies $(a, a) \in R$, so $I_S \subset R$.

Conversely, we prove if $I_S \subset R$, then R is reflexive.

Suppose $I_S \subset R$.

Let $x \in S$ be arbitrary.

Then $(x, x) \in S \times S$.

Since there is an element $x \in S$ such that $(x, x) \in S \times S$, then $(x, x) \in I_S$.

Since $I_S \subset R$, then $(x, x) \in R$.

Therefore, R is reflexive. □

Proposition 3. *A relation R on a set S is symmetric iff $R = R^{-1}$.*

Proof. Let R be a relation on a set S.

We must prove R is symmetric iff $R = R^{-1}$.

We prove if R is symmetric, then $R = R^{-1}$.

Suppose R is symmetric.

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

Since R is symmetric and $(a, b) \in R$, then $(b, a) \in R$.

Since $(b, a) \in R$ iff $(a, b) \in R^{-1}$, then $(a, b) \in R^{-1}$.

Hence, $(a, b) \in R$ implies $(a, b) \in R^{-1}$, so $R \subset R^{-1}$.

Let $(c, d) \in R^{-1}$.

Then, by definition of $R^{-1}, (d, c) \in R$.

Since R is symmetric and $(d, c) \in R$, then $(c, d) \in R$.

Hence, $(c, d) \in R^{-1}$ implies $(c, d) \in R$, so $R^{-1} \subset R$.

Since $R \subset R^{-1}$ and $R^{-1} \subset R$, then $R = R^{-1}$.

Conversely, we prove if $R = R^{-1}$, then R is symmetric.

Suppose $R = R^{-1}$.

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

Since $R = R^{-1}$, then $(a, b) \in R^{-1}$.

Since $(a, b) \in R^{-1}$ iff $(b, a) \in R$, then $(b, a) \in R$.

Hence, $(a, b) \in R$ implies $(b, a) \in R$, so R is symmetric. □

Proposition 4. *Let r and s be relations.*
Then $r \circ s \subset dom\ s \times rng\ r$.

Proof. Suppose $(a, b) \in r \circ s$.
Then there exists c such that $(a, c) \in s$ and $(c, b) \in r$.
Since $(a, c) \in s$, then $a \in dom$ s.
Since $(c, b) \in r$, then $b \in rng$ r.
Since $a \in dom$ s and $b \in rng$ r, then $(a, b) \in dom$ s $\times$ rng r.
Therefore, $r \circ s \subset dom$ s $\times$ rng r. □

Equivalence Relations

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

Proof. We prove 1.
Let $a \in S$.
Since $\sim$ is an equivalence relation, then $\sim$ is reflexive, so $a \sim a$.
Since $a \in S$ and $a \sim a$, then by definition of equivalence class, $a \in [a]$. □

Proof. We prove 2.
Let $a, b \in S$.
Observe that

$$\begin{aligned} a \in [b] &\Leftrightarrow a \in S \wedge a \sim b \\ &\Leftrightarrow a \sim b. \end{aligned}$$

□

Proof. We prove 3.
Let $a, b \in S$.
We prove if $[a] = [b]$, then $a \sim b$.
Suppose $[a] = [b]$.
By statement 1, we know that $a \in [a]$.
Since $a \in [a]$ and $[a] = [b]$, then $a \in [b]$.
Therefore, by statement 2 of the theorem, we conclude $a \sim b$.

Conversely, we prove if $a \sim b$, then $[a] = [b]$.
Suppose $a \sim b$.
We first prove $[a] \subset [b]$.
Let $x \in [a]$.
Then $x \in S$ and $x \sim a$.
Since $x \sim a$ and $a \sim b$, then $x \sim b$.
Since $x \in S$ and $x \sim b$, then $x \in [b]$.
Therefore, $x \in [a]$ implies $x \in [b]$, so $[a] \subset [b]$.

We next prove $[b] \subset [a]$.
Let $y \in [b]$.
Then $y \in S$ and $y \sim b$.
Since $a \sim b$, then $b \sim a$.
Since $y \sim b$ and $b \sim a$, then $y \sim a$.
Since $y \in S$ and $y \sim a$, then $y \in [a]$.
Therefore, $y \in [b]$ implies $y \in [a]$, so $[b] \subset [a]$.
Since $[a] \subset [b]$ and $[b] \subset [a]$, then $[a] = [b]$, as desired. $\square$

Proof. We prove 4.
Let $a, b \in S$.
To prove either $[a] = [b]$ or $[a] \cap [b] = \emptyset$, we prove $[a] \cap [b] \neq \emptyset$ implies $[a] = [b]$.

Suppose $[a] \cap [b] \neq \emptyset$.
Then $[a] \cap [b]$ is not empty, so there exists an element in $[a] \cap [b]$.
Let c be some element in $[a] \cap [b]$.
Then $c \in [a]$ and $c \in [b]$.
Since $c \in [a]$, then by statement 2, we know that $c \sim a$.
Since $c \in [b]$, then b y statement 2, we know that $c \sim b$.
Since $c \sim a$, then $a \sim c$.
Since $a \sim c$ and $c \sim b$, then $a \sim b$.
By statement 3 we conclude $[a] = [b]$, as desired. $\square$

Proof. We prove 5.
Let $x \in \cup([a] : a \in S)$.
Then there exists $a \in S$ such that $x \in [a]$.
Since $[a] = \{s \in S : s \sim a\}$, then $[a] \subset S$.
Since $x \in [a]$ and $[a] \subset S$, then $x \in S$.
Hence, $x \in \cup([a] : a \in S)$ implies $x \in S$, so $\cup([a] : a \in S) \subset S$.

Let $y \in S$.
By statement one, we know that $y \in [y]$.
Hence, there exists some $a \in S$ such that $y \in [a]$, so $y \in \cup([a] : a \in S)$.
Thus, $y \in S$ implies $y \in \cup([a] : a \in S)$, so $S \subset \cup([a] : a \in S)$.
Since $\cup([a] : a \in S) \subset S$ and $S \subset \cup([a] : a \in S)$, then $\cup([a] : a \in S) = S$. $\square$

Corollary 6. *Let $\sim$ be an equivalence relation on set S.*
Then each element of S is an element of exactly one equivalence class.

Proof. Let x be an arbitrary element of S.
Since $\sim$ is an equivalence relation, then by the previous theorem, $x \in [x]$.
Therefore, x is in at least one equivalence class.

Suppose there exist equivalence classes $[a]$ and $[b]$ such that $x \in [a]$ and $x \in [b]$.
Since $x \in [a]$, then $x \sim a$.
Since $x \in [b]$, then $x \sim b$.
Since $x \sim a$, then $a \sim x$.
Since $a \sim x$ and $x \sim b$, then $a \sim b$.
By the previous theorem, we conclude $[a] = [b]$.
Therefore, x is in at most one equivalence class.

Since x is in at least one equivalence class and x is in at most one equivalence class, then x is in exactly one equivalence class. □

Theorem 7. ***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.

Proof. We prove $\sim$ is an equivalence relation on S.
Let $a \in S$.
Then by condition 3 in the definition of partition, there exists $T \in P$ such that $a \in T$.
Hence, there exists $T \in P$ such that $a \in T$ and $a \in T$, so $a \sim a$.
Therefore, $\sim$ is reflexive.

Let $a, b \in S$ such that $a \sim b$.
Then there exists $T \in P$ such that $a \in T$ and $b \in T$.
Hence, there exists $T \in P$ such that $b \in T$ and $a \in T$.
Thus, $b \sim a$.
Hence, $a \sim b$ implies $b \sim a$, so $\sim$ is symmetric.
Let $a, b, c \in S$ such that $a \sim b$ and $b \sim c$.
Then there exists $V \in P$ such that $a \in V$ and $b \in V$ and there exists $W \in P$ such that $b \in W$ and $c \in W$.
To prove $a \sim c$, we must prove there exists $T \in P$ such that $a \in T$ and $c \in T$.
Since $b \in V$ and $b \in W$, then $b \in V \cap W$, so $V \cap W \neq \emptyset$.
By condition 2 in the definition of partition of a set, either $V = W$ or $V \cap W = \emptyset$. Hence, $V = W$.

Let T be the set $V = W$.
Then $T = V = W$.
Since $a \in V$ and $V = T$, then $a \in T$.
Since $c \in W$ and $W = T$, then $c \in T$.
Hence, there exists $T \in P$ such that $a \in T$ and $c \in T$, so $a \sim c$.
Thus, $a \sim b$ and $b \sim c$ imply $a \sim c$, so $\sim$ is transitive.
Therefore, $\sim$ is an equivalence relation on S. □

Theorem 8. ***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.

Solution.

Our hypothesis is
1. S is a nonempty set.
2. $\sim$ is an equivalence relation on S.

Our conclusion is $\frac{S}{\sim} = \{[x] : x \in S\}$ is a partition of S.

To prove $\frac{S}{\sim}$ is a partition of S, we must prove:
1. $(\forall T \in \frac{S}{\sim})(T \subset S)$.
2. $(\forall T \in \frac{S}{\sim})(T \neq \emptyset)$.
3. for all $T_1, T_2 \in \frac{S}{\sim}$, either $T_1 = T_2$ or $T_1 \cap T_2 = \emptyset$.
4. $(\forall x \in S)(\exists T \in \frac{S}{\sim})(x \in T)$.

By hypothesis $\sim$ is an equivalence relation, so $\sim$ is reflexive, symmetric, and transitive. □

Proof. Let $\frac{S}{\sim}$ be the collection of all equivalence classes of $\sim$. Then $\frac{S}{\sim} = \{[x] : x \in S\}$.

Since S is not empty, then there is an element of S.
Let a be some element of S.
Since $a \in S$ and $\sim$ is an equivalence relation on S, then $a \in [a]$.
Thus, $[a] \in \frac{S}{\sim}$, so $\frac{S}{\sim}$ is not empty.
Let $T \in \frac{S}{\sim}$.
Then there exists $a \in S$ such that $T = [a]$.
Since $[a] = \{x \in S : a \sim x\}$, then $[a] \subset S$, so $T \subset S$.
Since $a \in S$ and $\sim$ is an equivalence relation on S, then $a \in [a]$.
Hence, $[a] \neq \emptyset$, so $T \neq \emptyset$.
Therefore, T is a nonempty subset of S, so every element of $\frac{S}{\sim}$ is a nonempty subset of S.

We prove for all $T_1, T_2 \in \frac{S}{\sim}$, either $T_1 = T_2$ or $T_1 \cap T_2 = \emptyset$.
Let $T_1, T_2 \in \frac{S}{\sim}$.
Then there exists $a \in S$ such that $T_1 = [a]$ and there exists $b \in S$ such that $T_2 = [b]$.

Since $\sim$ is an equivalence relation on S and $a \in S$ and $b \in S$, then either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Hence, either $T_1 = T_2$ or $T_1 \cap T_2 = \emptyset$.

We prove for every $x \in S$, there exists $T \in \frac{S}{\sim}$ such that $x \in T$.

Let $x \in S$.

Since $\sim$ is an equivalence relation on S, then $x \in [x]$.

Let $T = [x]$.

Then $x \in T$.

Since $x \in S$, then $[x] \in \frac{S}{\sim}$, so $T \in \frac{S}{\sim}$.

Thus, there exists $T \in \frac{S}{\sim}$ such that $x \in T$.

Hence, each element of S lies in at least one element of $\frac{S}{\sim}$.

Therefore, $\frac{S}{\sim}$ is a partition of S. □

Theorem 9. *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 $\frac{S}{\frac{S}{P}} = P$.

Proof. Suppose R is an equivalence relation on a set S.

Then $\frac{S}{R}$, the collection of all equivalence classes induced by R, is a partition of S.

Therefore, $\frac{S}{\frac{S}{R}}$ is an equivalence relation on S defined by $(a, b) \in \frac{S}{\frac{S}{R}}$ iff there exists a cell $T \in \frac{S}{R}$ such that $a \in T$ and $b \in T$ for all $a, b \in S$.

To prove $\frac{S}{\frac{S}{R}} = R$, we prove $\frac{S}{\frac{S}{R}} \subset R$ and $R \subset \frac{S}{\frac{S}{R}}$.

Let $(x, y) \in \frac{S}{\frac{S}{R}}$.

Then $x \in S$ and $y \in S$ and there exists a cell $T \in \frac{S}{R}$ such that $x \in T$ and $y \in T$.

Each element of $\frac{S}{R}$ is an equivalence class of R, so T is an equivalence class of R.

Since x is in exactly one equivalence class of R and $x \in [x]$ and $x \in T$, then $[x] = T$.

Since y is in exactly one equivalence class of R and $y \in [y]$ and $y \in T$, then $[y] = T$.

Therefore, $[x] = T = [y]$, so xRy.

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

Thus, $(x, y) \in \frac{S}{\frac{S}{R}}$ implies $(x, y) \in R$, so $\frac{S}{\frac{S}{R}} \subset R$.

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

Then xRy, so $[x] = [y]$.

Let $T = [x] = [y]$.

Then $T \in \frac{S}{R}$ and $x \in [x]$ and $y \in [y]$.

Thus, there exists a cell T in the partition $\frac{S}{R}$ such that $x \in T$ and $y \in T$, so $(x, y) \in \frac{S}{\frac{S}{R}}$.

Hence, $(x,y) \in R$ implies $(x,y) \in \frac{S}{\frac{S}{R}}$, so $R \subset \frac{S}{\frac{S}{R}}$.

Since $\frac{S}{\frac{S}{R}} \subset R$ and $R \subset \frac{S}{\frac{S}{R}}$, then $\frac{S}{\frac{S}{R}} = R$. $\square$

Proof. We prove if P is a partition of set S, then $\frac{S}{\frac{S}{P}} = P$.

Suppose P is a partition of S.

Then $\frac{S}{P}$ defined by $(a,b) \in \frac{S}{P}$ iff there exists a cell $T \in P$ such that $a \in T$ and $b \in T$ for all $a, b \in S$ is an equivalence relation on S.

Thus, $\frac{S}{\frac{S}{P}} = \{[x] : x \in S\}$, the collection of all equivalence classes induced by $\frac{S}{P}$, is a partition of S.

To prove $\frac{S}{\frac{S}{P}} = P$, we prove $\frac{S}{\frac{S}{P}} \subset P$ and $P \subset \frac{S}{\frac{S}{P}}$.

We first prove $P \subset \frac{S}{\frac{S}{P}}$.

Let $T \in P$.

To prove $T \in \frac{S}{\frac{S}{P}}$, we must show there exists $x \in S$ such that $T = [x]$.

Since $T \in P$, then $T \subset S$ and by condition 1 in the definition of partition, $T \neq \emptyset$.

Thus, T is not empty, so there is an element in T.

Let x be an element of T.

Since $x \in T$ and $T \subset S$, then $x \in S$.

To prove $T = [x]$, we prove $T \subset [x]$ and $[x] \subset T$.

Observe that $[x] = \{s \in S : (x,s) \in \frac{S}{P}\} = \{s \in S : (\exists T' \in P)(x \in T' \wedge s \in T')\}$.

We prove $T \subset [x]$.

Let $t \in T$.

To prove $t \in [x]$, we must prove $t \in S$ and there exists a cell T' such that $x \in T'$ and $t \in T'$.

Since $t \in T$ and $T \subset S$, then $t \in S$.

Let $T' = T$.

Then $x \in T'$ since $x \in T$ and $t \in T'$ since $t \in T$.

Hence, $t \in [x]$.

Thus, $t \in T$ implies $t \in [x]$, so $T \subset [x]$.

We prove $[x] \subset T$.

Let $s \in [x]$. We must prove $s \in T$.

Since $s \in [x]$, then $s \in S$ and there exists a cell $T' \in P$ such that $x \in T'$ and $s \in T'$.

Since $x \in T$ and $x \in T'$, then $x \in T \cap T'$.

Thus, $T \cap T' \neq \emptyset$.

By condition 2 in the definition of partition, either $T = T'$ or $T \cap T' = \emptyset$.

Hence, $T = T'$.

Since $s \in T'$ and $T' = T$, then $s \in T$.

Thus, $s \in [x]$ implies $s \in T$, so $[x] \subset T$.

Since $T \subset [x]$ and $[x] \subset T$, then $T = [x]$.
Therefore, there exists $x \in S$ such that $T = [x]$, so $T \in \frac{S}{\frac{S}{P}}$.
Thus, $T \in P$ implies $T \in \frac{S}{\frac{S}{P}}$, so $P \subset \frac{S}{\frac{S}{P}}$.

We now prove $\frac{S}{\frac{S}{P}} \subset P$.
Let $T \in \frac{S}{\frac{S}{P}}$.
Then there exists $x \in S$ such that $T = [x]$.
We must prove $T \in P$.
Since $x \in [x]$ and $[x] = T$, then $x \in T$.
Since $x \in [x]$, then by definition of $[x]$, there exists $T' \in P$ such that $x \in T'$.
Thus, $x \in T$ and $x \in T'$, so $x \in T \cap T'$.
Hence, $T \cap T' \neq \emptyset$.
By condition 2 in the definition of partition, either $T = T'$ or $T \cap T' = \emptyset$.
Thus, $T = T'$.
Since $T = T'$ and $T' \in P$, then $T \in P$.
Hence, $T \in \frac{S}{\frac{S}{P}}$ implies $T \in P$, so $\frac{S}{\frac{S}{P}} \subset P$.
Since $\frac{S}{\frac{S}{P}} \subset P$ and $P \subset \frac{S}{\frac{S}{P}}$, then $\frac{S}{\frac{S}{P}} = P$. $\square$

Proposition 10. *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.*

Proof. Suppose E_1 and E_2 are equivalence relations on a set S.
Let $R = E_1 \cap E_2$.
Since $E_1 \cap E_2 \subset E_1$ and $E_1 \subset S \times S$, then $E_1 \cap E_2 \subset S \times S$.
Thus, $R \subset S \times S$, so R is a relation on S.

Reflexive:
Let $x \in S$.
Since E_1 is reflexive, then $(x, x) \in E_1$.
Since E_2 is reflexive, then $(x, x) \in E_2$.
Thus, $(x, x) \in E_1$ and $(x, x) \in E_2$, so $(x, x) \in E_1 \cap E_2$.
Hence, $(x, x) \in R$.
Therefore, R is reflexive.

Symmetric:
Let $x, y \in S$ such that $(x, y) \in R$.
Since $R = E_1 \cap E_2$, then $(x, y) \in E_1$ and $(x, y) \in E_2$.
Since E_1 is symmetric and $(x, y) \in E_1$, then $(y, x) \in E_1$.
Since E_2 is symmetric and $(x, y) \in E_2$, then $(y, x) \in E_2$.
Thus, $(y, x) \in E_1$ and $(y, x) \in E_2$, so $(y, x) \in E_1 \cap E_2$.
Hence, $(y, x) \in R$.
Therefore, $(x, y) \in R$ implies $(y, x) \in R$, so R is symmetric.

Transitive:

Let $x, y, z \in S$ such that $(x, y) \in R$ and $(y, z) \in R$.

Since $R = E_1 \cap E_2$, then $(x, y) \in E_1$ and $(x, y) \in E_2$ and $(y, z) \in E_1$ and $(y, z) \in E_2$.

Since E_1 is transitive and $(x, y) \in E_1$ and $(y, z) \in E_1$, then $(x, z) \in E_1$.

Since E_2 is transitive and $(x, y) \in E_2$ and $(y, z) \in E_2$, then $(x, z) \in E_2$.

Thus, $(x, z) \in E_1$ and $(x, z) \in E_2$, so $(x, z) \in E_1 \cap E_2 = R$.

Therefore, $(x, y) \in R$ and $(y, z) \in R$ implies $(x, z) \in R$, so R is transitive.

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

Therefore, $E_1 \cap E_2$ is an equivalence relation on S. □

Theorem 11. *Let $\sim$ be an equivalence relation on 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.

Solution. We must prove f is a function and f is surjective.

To prove f is a function, we must prove:

1. Existence: $f(a) \in \frac{S}{\sim}$.
2. Uniqueness: if $a_1, a_2 \in S$ such that $a_1 = a_2$, then $f(a_1) = f(a_2)$. □

Proof. Let $a \in S$.

Then $f(a) = [a]$.

Hence, there exists $a \in S$ such that $f(a) = [a]$.

Therefore, $f(a) \in \frac{S}{\sim}$.

Let $a_1, a_2 \in S$ such that $a_1 = a_2$.

Since $\sim$ is an equivalence relation on S, then $\sim$ is reflexive.

Thus, $a_1 \sim a_1$.

Hence, $a_1 \sim a_2$.

Therefore, $[a_1] = [a_2]$.

Observe that

$$\begin{aligned} f(a_1) &= [a_1] \\ &= [a_2] \\ &= f(a_2). \end{aligned}$$

Thus, $a_1 = a_2$ implies $f(a_1) = f(a_2)$, so f is well defined.

Therefore, f is a function.

Let $[b] \in \frac{S}{\sim}$.
Then $b \in S$.
Thus, $f(b) = [b]$.
Hence, there exists $b \in S$ such that $f(b) = [b]$.
Therefore, f is surjective. □

Theorem 12. *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 $x_1, x_2 \in S$.

Proof. Let $x_1, x_2 \in S$.
Since f is the natural projection of S onto $\frac{S}{\sim}$, then $f(x_1) = [x_1]$ and $f(x_2) = [x_2]$.
Observe that

$$\begin{aligned} x_1 \sim x_2 &\Leftrightarrow [x_1] = [x_2] \\ &\Leftrightarrow f(x_1) = f(x_2). \end{aligned}$$

□

Proposition 13. *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.

Proof. Let $a \in A$.
Then $f(a) = f(a)$.
Since $f(a) = f(a)$ iff $a \sim a$, then $a \sim a$.
Hence, $\sim$ is reflexive.

Let $a, b \in A$ such that $a \sim b$.
Then $f(a) = f(b)$, so $f(b) = f(a)$.
Since $f(b) = f(a)$ iff $b \sim a$, then $b \sim a$.
Hence, $a \sim b$ implies $b \sim a$, so $\sim$ is symmetric.

Let $a, b, c \in A$ such that $a \sim b$ and $b \sim c$.
Then $f(a) = f(b)$ and $f(b) = f(c)$.
Thus, $f(a) = f(b) = f(c)$, so $f(a) = f(c)$.
Since $f(a) = f(c)$ iff $a \sim c$, then $a \sim c$.
Therefore, $a \sim b$ and $b \sim c$ imply $a \sim c$, so $\sim$ is transitive.
Since $\sim$ is reflexive, symmetric, and transitive, then $\sim$ is an equivalence relation on A. □

Theorem 14. *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 $b \in f(A)$.

Proof. Since the kernel of f is an equivalence relation on A, then the quotient set of A under $\ker f$ exists.

Let $\frac{A}{\ker f}$ be the quotient set of A under $\ker f$.

Then $\frac{A}{\ker f} = \{[x] : x \in A\}$.

Since f is a function, then the image of A under f exists.

Let $f(A)$ be the image of A under f.

Then $f(A) = \{f(x) \in B : x \in A\}$.

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

We prove g is a function.

Let $[x] \in \frac{A}{\ker f}$.

Then $x \in A$ and $g([x]) = f(x)$.

Since f is a function, then $f(x) \in B$.

Thus, there exists $x \in A$ such that $f(x) \in B$, so $f(x) \in f(A)$.

Hence, $g([x]) \in f(A)$.

Let $[x_1], [x_2] \in \frac{A}{\ker f}$ such that $[x_1] = [x_2]$.

Then $x_1, x_2 \in A$.

Since $\ker f$ is an equivalence relation on A, then $[x_1] = [x_2]$ iff $x_1 \sim x_2$ and $x_1 \sim x_2$ iff $f(x_1) = f(x_2)$.

Thus, $[x_1] = [x_2]$ iff $f(x_1) = f(x_2)$.

Hence, $f(x_1) = f(x_2)$.

Observe that

$$\begin{aligned} g([x_1]) &= f(x_1) \\ &= f(x_2) \\ &= g([x_2]). \end{aligned}$$

Therefore, $[x_1] = [x_2]$ implies $g([x_1]) = g([x_2])$, so g is well defined.

Therefore, g is a function.

Let $f(x) \in f(A)$.

Then there exists $x \in A$ such that $f(x) \in B$.

Since $x \in A$, then $[x] \in \frac{A}{\ker f}$.

Thus, $g([x]) = f(x)$.

Hence, there exists $[x] \in \frac{A}{\ker f}$ such that $g([x]) = f(x)$.

Therefore, g is surjective.

Let $[a], [b] \in \frac{A}{\ker f}$ such that $g([a]) = g([b])$.

Then $a, b \in A$ and $f(a) = f(b)$.

Since $f(a) = f(b)$ iff $a \sim b$ and $a \sim b$ iff $[a] = [b]$, then $f(a) = f(b)$ iff $[a] = [b]$.

Thus, $[a] = [b]$.

Hence, $g([a]) = g([b])$ implies $[a] = [b]$, so g is injective.

Since g is a surjective and injective, then g is bijective.
Therefore, g is a bijection from $\frac{A}{\ker f}$ to $f(A)$.

We prove the pre image of each element in $f(A)$ is an equivalence class of A under $\ker f$.
Let $b \in f(A)$.
Then there exists $a \in A$ such that $f(a) = b$.
Let $f^{-1}(b)$ be the preimage of b.
Then $f^{-1}(b) = \{a \in A : f(a) = b\}$.

Let $x \in [a]$.
Then $x \in A$ and $x \sim a$.
Since $x \sim a$ iff $f(x) = f(a)$, then $f(x) = f(a)$.
Thus, $f(x) = f(a) = b$.
Hence, there exists $x \in A$ such that $f(x) = b$, so $x \in f^{-1}(b)$.
Therefore, $x \in [a]$ implies $x \in f^{-1}(b)$, so $[a] \subset f^{-1}(b)$.

Let $y \in f^{-1}(b)$.
Then $y \in A$ and $f(y) = b$.
Since $f(y) = b = f(a)$, then $f(y) = f(a)$.
Since $f(y) = f(a)$ iff $y \sim a$, then $y \sim a$.
Hence, $y \in A$ and $y \sim a$, so $y \in [a]$.
Thus, $y \in f^{-1}(b)$ implies $y \in [a]$, so $f^{-1}(b) \subset [a]$.
Since $[a] \subset f^{-1}(b)$ and $f^{-1}(b) \subset [a]$, then $[a] = f^{-1}(b)$.

Therefore, there exists $a \in A$ such that $[a] = f^{-1}(b)$.
Hence, $f^{-1}(b) \in \frac{A}{\ker f}$.
Thus, $f^{-1}(b)$ is an equivalence class of A under $\ker f$. □

Partial Orders

Proposition 15. *Any element of a partially ordered set is an upper and lower bound of $\emptyset$.*

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

Since the empty set is a subset of any set, then $\emptyset \subset S$. Since $(S, \leq)$ is a poset, then S is not empty.

Let $s \in S$.

To prove s is an upper bound of $\emptyset$, we must prove $x \leq s$ for all $x \in \emptyset$.

Since there is no element in $\emptyset$, then the statement there exists $x \in \emptyset$ such that $x \not\leq s$ is false. Hence, the statement $x \leq s$ for all $x \in \emptyset$ is true. Therefore, s is an upper bound of $\emptyset$, as desired.

To prove s is a lower bound of $\emptyset$, we must prove $s \leq x$ for all $x \in \emptyset$.

Since there is no element in $\emptyset$, then the statement there exists $x \in \emptyset$ such that $s \not\leq x$ is false. Hence, the statement $s \leq x$ for all $x \in \emptyset$ is true. Therefore, s is a lower bound of $\emptyset$, as desired. □

Theorem 16. ***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.

Proof. Suppose there is a greatest element of S. Let M be a greatest element of S.

To prove M is unique, suppose M_1 and M_2 are greatest elements of S. We must prove $M_1 = M_2$.

Since M_1 is a greatest element of S, then $M_1 \in S$ and $x \leq M_1$ for all $x \in S$. Since M_2 is a greatest element of S, then $M_2 \in S$ and $x \leq M_2$ for all $x \in S$. Since $M_2 \in S$ and $x \leq M_1$ for all $x \in S$, then $M_2 \leq M_1$. Since $M_1 \in S$ and $x \leq M_2$ for all $x \in S$, then $M_1 \leq M_2$. Since $\leq$ is antisymmetric and $M_1 \leq M_2$ and $M_2 \leq M_1$, then $M_1 = M_2$.

Therefore, M is unique. □

Theorem 17. ***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.

Proof. Suppose there is a least element of S. Let m be a least element of S.

To prove m is unique, suppose m_1 and m_2 are least elements of S. We must prove $m_1 = m_2$.

Since m_1 is a least element of S, then $m_1 \in S$ and $m_1 \leq x$ for all $x \in S$. Since m_2 is a least element of S, then $m_2 \in S$ and $m_2 \leq x$ for all $x \in S$. Since $m_2 \in S$ and $m_1 \leq x$ for all $x \in S$, then $m_1 \leq m_2$. Since $m_1 \in S$ and $m_2 \leq x$ for all $x \in S$, then $m_2 \leq m_1$. Since $\leq$ is antisymmetric and $m_1 \leq m_2$ and $m_2 \leq m_1$, then $m_1 = m_2$.

Therefore, m is unique. □

Theorem 18. ***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.

Proof. Suppose there is a least upper bound of S in P.

Let U be a least upper bound of S in P.

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

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

Since $B \subset P$ and U is the least element of B, then U is unique. □

Theorem 19. ***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.

Proof. Suppose there is a greatest lower bound of S in P.
Let L be a greatest lower bound of S in P.
Let B be the set of all lower bounds of S in P.
Then $B = \{u \in P : u \text{ is a lower bound of } S\}$.
Since $B \subset P$ and L is the greatest element of B, then L is unique. □

Theorem 20. ***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 $\inf S = \min S$.

Proof. We prove 1.
Suppose $\max S$ exists in P.
Since $\max S$ is an upper bound of S in P, then S has at least one upper bound in P.
Let M be an arbitrary upper bound of S in P.
Since M is an upper bound of S and $\max S \in S$, then $\max S \leq M$.
Hence, $\max S$ is the least upper bound of S in P.
Therefore, $\max S = \sup S$. □

Proof. We prove 2.
Suppose $\min S$ exists in P.
Since $\min S$ is a lower bound of S in P, then S has at least one lower bound in P.
Let M be an arbitrary lower bound of S in P.
Since M is a lower bound of S and $\min S \in S$, then $M \leq \min S$.
Hence, $\min S$ is the greatest lower bound of S in P.
Therefore, $\min S = \inf S$. □

Functions

Proposition 21. ***A function value is unique.***
Let f be a function.
Let $a, b \in dom f$.
If $a = b$, then $f(a) = f(b)$.

Proof. Suppose $a = b$.
Since $a \in dom f$ and f is a relation, then $(a, f(a)) \in f$.
Since $b \in dom f$ and f is a relation, then $(b, f(b)) \in f$.
Since $b = a$ and $(b, f(b)) \in f$, then $(a, f(b)) \in f$.
Since f is a function and $(a, f(a)) \in f$ and $(a, f(b)) \in f$, then $f(a) = f(b)$. □

Theorem 22. ***equality of functions***
Let f and g be functions.
Let $dom f$ 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 $x \in domf \cap domg$.

Proof. We prove if $domf = domg$ and $f(x) = g(x)$ for all $x \in domf \cap domg$, then $f = g$.

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

We first prove $f \subset g$.
Let $x \in domf$.
Then $(x, f(x)) \in f$.
Since $x \in domf$ and $domf = domg$, then $x \in domg$, so $(x, g(x)) \in g$.
Since $x \in domf$ and $x \in domg$, then $x \in domf \cap domg$, so $f(x) = g(x)$.
Hence, $(x, f(x)) \in g$.
Thus, if $(x, f(x)) \in f$, then $(x, f(x)) \in g$, so $f \subset g$.

We prove $g \subset f$.
Let $y \in domg$.
Then $(y, g(y)) \in g$.
Since $y \in domg$ and $domg = domf$, then $y \in domf$, so $(y, f(y)) \in f$.
Since $y \in domf$ and $y \in domg$, then $y \in domf \cap domg$, so $f(y) = g(y)$.
Hence, $(y, g(y)) \in f$.
Thus, if $(y, g(y)) \in g$, then $(y, g(y)) \in f$, so $g \subset f$.

Since $f \subset g$ and $g \subset f$, then $f = g$, as desired. □

Proof. Conversely, we prove if $f = g$, then $domf = domg$ and $f(x) = g(x)$ for all $x \in domf \cap domg$.

Suppose $f = g$.

We first prove $domf = domg$.
Let $x \in domf$.
Then $(x, f(x)) \in f$.
Since $f = g$, then $(x, f(x)) \in g$, so $x \in domg$.
Thus, $domf \subset domg$.

Let $y \in domg$.
Then $(y, g(y)) \in g$.
Since $g = f$, then $(y, g(y)) \in f$, so $y \in domf$.
Thus, $domg \subset domf$.

Since $domf \subset domg$ and $domg \subset domf$, then $domf = domg$, as desired.

We next prove $f(x) = g(x)$ for all $x \in domf \cap domg$.
Let $x \in domf \cap domg$.
Then $x \in domf$ and $x \in domg$, so $(x, f(x)) \in f$ and $(x, g(x)) \in g$.
Since $(x, g(x)) \in g$ and $g = f$, then $(x, g(x)) \in f$.
Since f is a function and $(x, f(x)) \in f$ and $(x, g(x)) \in f$, then $f(x) = g(x)$, as desired. □

Proposition 23. ***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* $x \in A$.

Proof. We prove if the maps $f : A \to B$ and $g : C \to D$ are equal, then $A = C$ and $B = D$ and $f(x) = g(x)$ for all $x \in A$.
Let $f : A \to B$ and $g : C \to D$ be equal maps.
Then $f = g$ and $B = D$.
Since $f = g$, then $domf = domg$ and $f(x) = g(x)$ for all $x \in domf \cap domg$.
Since $domf = domg$ and $domf = A$ and $domg = C$, then $A = C$.
Thus, $f(x) = g(x)$ for all $x \in A \cap C = A \cap A = A$.
Therefore, $A = C$ and $B = D$ and $f(x) = g(x)$ for all $x \in A$, as desired. □

Proof. Conversely, we prove if $A = C$ and $B = D$ and $f(x) = g(x)$ for all $x \in A$, then the maps $f : A \to B$ and $g : C \to D$ are equal.
Suppose $A = C$ and $B = D$ and $f(x) = g(x)$ for all $x \in A$.
Let $f : A \to B$ and $g : C \to D$ be maps.
Then f and g are functions and $domf = A$ and $domg = C$.
Since $domf = A = C = domg$, then $domf = domg$.

Let $x \in domf \cap domg$.
Then $x \in A \cap C$, so $x \in A$ and $x \in C$.
Thus, $x \in A$, so $f(x) = g(x)$.
Hence $f(x) = g(x)$ for all $x \in domf \cap domg$.
Since f and g are functions and $domf = domg$ and $f(x) = g(x)$ for all $x \in domf \cap domg$, then $f = g$.
Since $f = g$ and $B = D$, then the maps $f : A \to B$ and $g : C \to D$ are equal, as desired. □

Proposition 24. ***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.

Proof. Observe that $f|_S : S \to B$ is a relation.
Since $f : A \to B$ is a map, then f is a function.
Let $a \in S$ and $b, b' \in B$ such that $(a, b) \in f|_S$ and $(a, b') \in f|_S$.

Then $f|_S(a) = b$ and $f|_S(a) = b'$.
Since $a \in S$, then $f(a) = b$ and $f(a) = b'$.
Since f is a function, then $b = b'$.
Therefore, $f|_S$ is a function.

We prove $domf|_S = S$.
Since $f|_S : S \to B$ is a relation, then $domf|_S \subset S$.
Let $s \in S$.
Since $S \subset A$, then $s \in A$.
Since $f : A \to B$ is a map, then there exists $t \in B$ such that $f(s) = t$.
Since $s \in S$, then $f|_S(s) = f(s)$, so $f|_S(s) = t$.
Since $s \in S$ and there exists t such that $f|_S(s) = t$, then $s \in domf|_S$, so $S \subset domf|_S$.
Since $domf|_S \subset S$ and $S \subset domf|_S$, then $domf|_S = S$.

We prove $rngf|_S \subset B$.
Let $y \in rngf|_S$.
Then there exists $x \in S$ such that $f|_S(x) = y$.
Since $x \in S$, then $f|_S(x) = f(x)$, so $f(x) = y$.
Since $x \in S$ and $S \subset A$, then $x \in A$.
Since $f : A \to B$ is a map, then $f(x) \in B$, so $y \in B$.
Hence, $rngf|_S \subset B$.

Since $f|_S$ is a function and $domf|_S = S$ and $rngf|_S \subset B$, then $f|_S : S \to B$ is a map. □

Theorem 25. ***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 $x \in dom\ g \circ f$.

Proof. We prove 1.
Since f and g are relations, then $g \circ f = \{(a, b) : (\exists c)((a, c) \in f \wedge (c, b) \in g\}$, so $g \circ f$ is a relation.
Let $(a, b) \in g \circ f$ and $(a, b') \in g \circ f$.
Since $(a, b) \in g \circ f$, then there exists c such that $(a, c) \in f$ and $(c, b) \in g$.
Since $(a, b') \in g \circ f$, then there exists d such that $(a, d) \in f$ and $(d, b') \in g$.
Since f is a function and $(a, c) \in f$ and $(a, d) \in f$, then $c = d$.
Since $(d, b') \in g$, then $(c, b') \in g$.
Since g is a function and $(c, b) \in g$ and $(c, b') \in g$, then $b = b'$.
Therefore, $g \circ f$ is a function. □

Proof. We prove 2.
Observe that $dom\ \mathrm{g} \circ f = \{a : (\exists b)((a, b) \in g \circ f\}$.
Let $S = \{x \in domf : f(x) \in domg\}$.
We must prove $dom\ \mathrm{g} \circ f = S$.

Suppose $x \in dom$ g $\circ f$.
Then there exists y such that $(x, y) \in g \circ f$.
Thus, there exists z such that $(x, z) \in f$ and $(z, y) \in g$.
Since $(x, z) \in f$ and f is a function, then $x \in dom f$ and $f(x) = z$.
Since $(z, y) \in g$, then $z \in dom g$, so $f(x) \in dom g$.
Since $x \in dom f$ and $f(x) \in dom g$, then $x \in S$, so dom g $\circ f \subset S$.

Suppose $x \in S$.
Then $x \in dom f$ and $f(x) \in dom g$.
Let $z = f(x)$.
Since $x \in dom f$, then $(x, f(x)) \in f$, so $(x, z) \in f$.
Since $f(x) \in dom g$ and $f(x) = z$, then $z \in dom g$, so there exists y such that $(z, y) \in g$.
Since $(x, z) \in f$ and $(z, y) \in g$, then $(x, y) \in g \circ f$.
Thus, there exists y such that $(x, y) \in g \circ f$, so $x \in dom$ g $\circ f$.
Therefore, $S \subset dom$ g $\circ f$.

Since dom g $\circ f \subset S$ and $S \subset dom$ g $\circ f$, then dom g $\circ f = S$, as desired. □

Proof. We prove 3.
Let $x \in dom$ g $\circ f$.
Since $g \circ f$ is a function, then $(g \circ f)(x)$ exists.
Let $z = (g \circ f)(x)$.
Then $(x, z) \in g \circ f$, so there exists y such that $(x, y) \in f$ and $(y, z) \in g$.
Since f and g are functions, then $f(x) = y$ and $g(y) = z$.
Thus, $(g \circ f)(x) = z = g(y) = g(f(x))$, as desired. □

Theorem 26. ***Function composition is associative.***
Let f, g, h be functions.
Then $(f \circ g) \circ h = f \circ (g \circ h)$.

Proof. Since f and g are functions, then $f \circ g$ is a function.
Since h is a function, then $(f \circ g) \circ h$ is a function.
Since g and h are functions, then $g \circ h$ is a function.
Since f is a function, then $f \circ (g \circ h)$ is a function.

We first prove $dom(f \circ g) \circ h = dom f \circ (g \circ h)$.

Let $x \in dom(f \circ g) \circ h$.
Then $x \in dom h$ and $h(x) \in dom f \circ g$.
Since $h(x) \in dom f \circ g$, then $h(x) \in dom g$ and $g(h(x)) \in dom f$.
Since $x \in dom h$ and $h(x) \in dom g$, then $x \in dom g \circ h$.
Since $g(h(x)) \in dom f$, then $(g \circ h)(x) \in dom f$.
Since $x \in dom g \circ h$ and $(g \circ h)(x) \in dom f$, then $x \in dom f \circ (g \circ h)$.
Thus, $dom(f \circ g) \circ h \subset dom f \circ (g \circ h)$.

Let $y \in dom f \circ (g \circ h)$.
Then $y \in dom g \circ h$ and $(g \circ h)(y) \in dom f$.
Since $y \in dom g \circ h$, then $y \in dom h$ and $h(y) \in dom g$.
Since $(g \circ h)(y) \in dom f$, then $g(h(y)) \in dom f$.
Since $h(y) \in dom g$ and $g(h(y)) \in dom f$, then $h(y) \in dom f \circ g$.
Since $y \in dom h$ and $h(y) \in dom f \circ g$, then $y \in dom(f \circ g) \circ h$.
Thus, $dom f \circ (g \circ h) \subset dom(f \circ g) \circ h$.

Since $dom(f \circ g) \circ h \subset dom f \circ (g \circ h)$ and $dom f \circ (g \circ h) \subset dom(f \circ g) \circ h$, then $dom(f \circ g) \circ h = dom f \circ (g \circ h)$.

Let $x \in dom(f \circ g) \circ h \cap dom f \circ (g \circ h)$.
Then $x \in dom(f \circ g) \circ h \cap dom(f \circ g) \circ h = dom(f \circ g) \circ h$ and

$$\begin{aligned} [(f \circ g) \circ h](x) &= (f \circ g)(h(x)) \\ &= f[g(h(x))] \\ &= f[(g \circ h)(x)] \\ &= [f \circ (g \circ h)](x). \end{aligned}$$

Therefore, $[(f \circ g) \circ h](x) = [f \circ (g \circ h)](x)$ for all x in the common domain.

Since $dom(f \circ g) \circ h = dom f \circ (g \circ h)$ and $[(f \circ g) \circ h](x) = [f \circ (g \circ h)](x)$ for all x in the common domain, then $(f \circ g) \circ h = f \circ (g \circ h)$, as desired. □

Proposition 27. *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 $x \in A$.

Proof. Since $f : A \to B$ and $g : B \to C$ are maps, then f and g are functions, so $g \circ f$ is a function and $dom\ g \circ f = \{x \in dom f : f(x) \in dom g\}$ and $(g \circ f)(x) = g(f(x))$ for all $x \in dom\ g \circ f$.
Since $dom f = A$ and $dom g = B$ and $dom\ g \circ f = \{x \in dom f : f(x) \in dom g\}$, then $dom\ g \circ f = \{x \in A : f(x) \in B\}$, so $dom\ g \circ f \subset A$.

Let $x \in A$.
Since $f : A \to B$ is a map, then $f(x) \in B$.
Since $x \in A$ and $f(x) \in B$, then $x \in dom\ g \circ f$.
Hence, $A \subset dom\ g \circ f$.

Since $dom\ g \circ f \subset A$ and $A \subset dom\ g \circ f$, then $dom\ g \circ f = A$.

Since $(g \circ f)(x) = g(f(x))$ for all $x \in dom\ g \circ f$, then $(g \circ f)(x) = g(f(x))$ for all $x \in A$.

We prove $rng\ \mathrm{g} \circ f \subset C$.

Let $y \in rng\ \mathrm{g} \circ f$.

Then there exists x such that $(x, y) \in g \circ f$.

Since $(x, y) \in g \circ f$, then $x \in dom\ \mathrm{g} \circ f$, so $x \in A$.

Since $g \circ f$ is a function and $(x, y) \in g \circ f$, then $(g \circ f)(x) = y$, so $y = (g \circ f)(x) = g(f(x))$.

Since $f : A \to B$ is a map and $x \in A$, then $f(x) \in B$.

Since $g : B \to C$ is a map, then $g(f(x)) \in C$.

Thus, $y \in C$, so $rng\ \mathrm{g} \circ f \subset C$.

Since $g \circ f$ is a function and $dom\ \mathrm{g} \circ f = A$ and $rng\ \mathrm{g} \circ f \subset C$, then $g \circ f : A \to C$ is a map. □

Proposition 28. *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 $f \circ I_A = I_B \circ f = f$.

Proof. We prove $f \circ I_A = f$.

Since $I_A : A \to A$ is a map and $f : A \to B$ is a map, then $f \circ I_A : A \to B$ is a map and $(f \circ I_A)(x) = f(I_A(x))$ for all $x \in A$.

Since the domain of $f \circ I_A$ and f is A, then $f \circ I_A$ and f have the same domain.

Since the codomain of $f \circ I_A$ and f is B, then $f \circ I_A$ and f have the same codomain.

Let $x \in A$.

Then $(f \circ I_A)(x) = f(I_A(x)) = f(x)$, so $(f \circ I_A)(x) = f(x)$ for all $x \in A$.

Therefore, $f \circ I_A = f$. □

Proof. We prove $I_B \circ f = f$.

Since $f : A \to B$ is a map and $I_B : B \to B$ is a map, then $I_B \circ f : A \to B$ is a map and $(I_B \circ f)(x) = I_B(f(x))$ for all $x \in A$.

Since the domain of $I_B \circ f$ and f is A, then $I_B \circ f$ and f have the same domain.

Since the codomain of $I_B \circ f$ and f is B, then $I_B \circ f$ and f have the same codomain.

Let $x \in A$.

Then $(I_B \circ f)(x) = I_B(f(x)) = f(x)$, so $(I_B \circ f)(x) = f(x)$ for all $x \in A$.

Therefore, $I_B \circ f = f$.

Since $f \circ I_A = f$ and $I_B \circ f = f$, then $f \circ I_A = f = I_B \circ f$, as desired. □

Theorem 29. ***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 $g = h$.

Proof. We prove if f is injective, then 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 $g = h$.

Suppose f is injective.

Let W be a set and let $g : W \to X$ and $h : W \to X$ be maps such that $f \circ g = f \circ h$.

We must prove $g = h$.

Since $g : W \to X$ is a map and $h : W \to X$ is a map, then $dom g = W = dom h$.

Let $x \in W$.

Since $f \circ g = f \circ h$, then $(f \circ g)(x) = (f \circ h)(x)$, so $f(g(x)) = f(h(x))$.

Since f is injective, then $g(x) = h(x)$.

Thus, $g(x) = h(x)$ for all $x \in W$, so $g = h$, as desired. □

Proof. Conversely, we prove if for every set W and every map $g : W \to X$ and $h : W \to X$ such that $f \circ g = f \circ h$ implies $g = h$, then f is injective.

We prove by contrapositive.

Suppose f is not injective.

We must prove there exists a set W and there exist maps $g : W \to X$ and $h : W \to X$ such that $f \circ g = f \circ h$ and $g \neq h$.

Since f is not injective, then there exist $a, b \in X$ such that $a \neq b$ and $f(a) = f(b)$.

Let $W = \{a, b\}$.

Let $g = \{(a, a), (b, a)\}$.

Then g is a function and $dom g = \{a, b\} = W$ and $rng g = \{a\} \subset X$.

Thus, $g : W \to X$ is a map and $g(a) = a = g(b)$.

Let $h = \{(a, b), (b, b)\}$.

Then h is a function and $dom h = \{a, b\} = W$ and $rng h = \{b\} \subset X$.

Thus, $h : W \to X$ is a map and $h(a) = b = h(b)$.

Since $(a, a) \in h$ iff $a = b$ and $a \neq b$, then $(a, a) \notin h$.

Since $(a, a) \in g$, but $(a, a) \notin h$, then $g \neq h$.

Since $g : W \to X$ is a map and $f : X \to Y$ is a map, then $f \circ g : W \to Y$ is a map and $(f \circ g)(x) = f(g(x))$ for all $x \in W$.

Since $h : W \to X$ is a map and $f : X \to Y$ is a map, then $f \circ h : W \to Y$ is a map and $(f \circ h)(x) = f(h(x))$ for all $x \in W$.

Observe that $dom(f \circ g) = W = dom(f \circ h)$.

Observe that $(f \circ g)(a) = f(g(a)) = f(a) = f(b) = f(h(a)) = (f \circ h)(a)$.

Observe that $(f \circ g)(b) = f(g(b)) = f(a) = f(b) = f(h(b)) = (f \circ h)(b)$.

Since $dom(f \circ g) = W = dom(f \circ h)$ and $(f \circ g)(a) = (f \circ h)(a)$ and $(f \circ g)(b) = (f \circ h)(b)$, then $f \circ g = f \circ h$. □

Proposition 30. *A map $f : A \to B$ is surjective iff $(\forall b \in B)(\exists a \in A)(f(a) = b)$.*

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

We first prove if f is surjective, then $(\forall b \in B)(\exists a \in A)(f(a) = b)$.

Suppose f is surjective.

Let $b \in B$.

Since f is surjective, then $rngf = B$.
Since $b \in B$, then $b \in rngf$, so there exists $a \in A$ such that $f(a) = b$.

Conversely, we prove if $(\forall b \in B)(\exists a \in A)(f(a) = b)$, then f is surjective.
Suppose $(\forall b \in B)(\exists a \in A)(f(a) = b)$.
Since $f : A \to B$ is a map, then $rngf \subset B$.
We prove $B \subset rngf$.
Suppose $b \in B$.
Then there exists $a \in A$ such that $f(a) = b$.
Hence, $b \in rngf$, so $B \subset rngf$.
Since $rngf \subset B$ and $B \subset rngf$, then $rngf = B$, so f is surjective. □

Theorem 31. ***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 $g = h$.

Proof. We prove if f is surjective, then 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 $g = h$.
Suppose f is surjective.
Let Z be a set and let $g : Y \to Z$ and $h : Y \to Z$ be maps such that $g \circ f = h \circ f$.
We must prove $g = h$.
Since $g : Y \to Z$ is a map and $h : Y \to Z$ is a map, then g and h are functions and $domg = Y = domh$ and the codomain of g is Z which is the codomain of h.
Since $X \neq \emptyset$ and $f : X \to Y$ is a map, then there exists $x \in X$, so $f(x) \in Y$.
Hence, $Y \neq \emptyset$.
Let $y \in Y$.
Since f is surjective, then there exists $x \in X$ such that $f(x) = y$.
Since $g \circ f = h \circ f$ and $x \in X$, then $(g \circ f)(x) = (h \circ f)(x)$.
Observe that

$$\begin{aligned} g(y) &= g(f(x)) \\ &= (g \circ f)(x) \\ &= (h \circ f)(x) \\ &= h(f(x)) \\ &= h(y). \end{aligned}$$

Therefore, $g(y) = h(y)$ for all $y \in Y$, so $g = h$, as desired. □

Proof. Conversely, we prove if for every set Z and every map $g : Y \to Z$ and $h : Y \to Z$ such that $g \circ f = h \circ f$ implies $g = h$, then f is surjective.
We prove by contrapositive.
Suppose f is not surjective.

We must prove there exists a set Z and there exist maps $g : Y \to Z$ and $h : Y \to Z$ such that $g \circ f = h \circ f$ and $g \neq h$.
Since f is not surjective, then there exists $y_0 \in Y$ such that for all $x \in X$, $f(x) \neq y_0$.
Since $X \neq \emptyset$, then there exists $x_0 \in X$.
Since $f : X \to Y$ is a map, then $f(x_0) \in Y$.
Let $Z = Y$.
Let $g : Y \to Z$ be the identity map on Y defined by $g(y) = y$.
Let $h : Y \to Z$ be a map defined by $h(y) = y$ if $y \neq y_0$ and $h(y_0) = f(x_0)$.

We prove $g \neq h$.
Since $x_0 \in X$, then $f(x_0) \neq y_0$.
Since $g(y_0) = y_0 \neq f(x_0) = h(y_0)$, then $g(y_0) \neq h(y_0)$, so $g \neq h$.

We prove $g \circ f = h \circ f$.
Since $f : X \to Y$ is a map and $g : Y \to Z$ is a map, then $g \circ f : X \to Z$ is a map and $(g \circ f)(x) = g(f(x))$ for all $x \in X$.
Since $f : X \to Y$ is a map and $h : Y \to Z$ is a map, then $h \circ f : X \to Z$ is a map and $(h \circ f)(x) = h(f(x))$ for all $x \in X$.
Observe that $dom(g \circ f) = X = dom(h \circ f)$.
Let $x \in X$.
Since $f : X \to Y$ is a map, then $f(x) \in Y$.
Since $x \in X$, then $f(x) \neq y_0$.
Observe that

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) \\ &= f(x) \\ &= h(f(x)) \\ &= (h \circ f)(x). \end{aligned}$$

Hence, $(g \circ f)(x) = (h \circ f)(x)$ for all $x \in X$.
Therefore, $g \circ f = h \circ f$, as desired. □

Proposition 32. ***identity map is bijective.***
Let S be a set.
The identity map $I_S : S \to S$ on S is a bijection.

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

We prove I_S is injective.
Let $a, b \in S$ such that $I_S(a) = I_S(b)$.
Then $a = b$.
Therefore, I_S is injective.

We prove I_S is surjective.
Let $b \in S$ be arbitrary.
Let $a = b$.
Then $a \in S$ and $I(a) = a = b$.
Thus, there exists $a \in S$ such that $I_S(a) = b$.
Therefore, I_S is surjective.
Since I_S is injective and surjective, then I_S is bijective, as desired. ☐

Theorem 33. *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.

Proof. We prove 1.
Suppose f and g are injective.
Since $f : A \to B$ is a map and $g : B \to C$ is a map, then $g \circ f : A \to C$ is a map.
Let $a, b \in A$ such that $(g \circ f)(a) = (g \circ f)(b)$.
Then $g(f(a)) = g(f(b))$.
Since g is injective, then $f(a) = f(b)$.
Since f is injective, then $a = b$.
Therefore, $g \circ f$ is injective. ☐

Proof. We prove 2.
Suppose f and g are surjective.
Since $f : A \to B$ is a map and $g : B \to C$ is a map, then $g \circ f : A \to C$ is a map.
Let $c \in C$ be arbitrary.
Since g is surjective, then there exists $b \in B$ such that $g(b) = c$.
Since f is surjective, then there exists $a \in A$ such that $f(a) = b$.
Observe that $(g \circ f)(a) = g(f(a)) = g(b) = c$.
Therefore, there exists $a \in A$ such that $(g \circ f)(a) = c$, so $g \circ f$ is surjective. ☐

Proof. We prove 3.
Suppose $g \circ f$ is injective.
Since $f : A \to B$ is a map and $g : B \to C$ is a map, then $g \circ f : A \to C$ is a map.
Let $a, b \in A$ such that $f(a) = f(b)$.
Then $(g \circ f)(a) = g(f(a)) = g(f(b)) = (g \circ f)(b)$, so $(g \circ f)(a) = (g \circ f)(b)$.
Since $g \circ f$ is injective, then $a = b$.
Therefore, f is injective. ☐

Proof. We prove 4.

Suppose $g \circ f$ is surjective.

Since $f : A \to B$ is a map and $g : B \to C$ is a map, then $g \circ f : A \to C$ is a map.

Let $c \in C$ be arbitrary.

Since $g \circ f$ is surjective, then there exists $a \in A$ such that $(g \circ f)(a) = c$.

Since $a \in A$ and $f : A \to B$ is a map, then $f(a) \in B$.

Observe that $g(f(a)) = (g \circ f)(a) = c$.

Thus, there exists $f(a) \in B$ such that $g(f(a)) = c$.

Therefore, g is surjective. □

Corollary 34. *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.

Proof. We prove 1.

Suppose f and g are bijective.

Since $f : A \to B$ is a map and $g : B \to C$ is a map, then $g \circ f : A \to C$ is a map.

Since f is bijective, then f is injective and surjective.

Since g is bijective, then g is injective and surjective.

Since f and g are injective, then $g \circ f$ is injective.

Since f and g are surjective, then $g \circ f$ is surjective.

Since $g \circ f$ is injective and surjective, then $g \circ f$ is bijective. □

Proof. We prove 2.

Suppose $g \circ f$ is bijective.

Then $g \circ f$ is injective and surjective.

Since $g \circ f$ is injective, then f is injective.

Since $g \circ f$ is surjective, then g is surjective. □

Theorem 35. ***existence of inverse function***

Let f be a function.

Then the inverse relation f^{-1} is a function iff f is injective.

Proof. We prove if f^{-1} is a function, then f is injective.

Suppose f^{-1} is a function.

Let $a_1, a_2 \in dom f$ such that $f(a_1) = f(a_2)$.

Since f is a relation, then $(a_1, f(a_1)) \in f$ and $(a_2, f(a_2)) \in f$.

Since f^{-1} is an inverse of f, then $(f(a_1), a_1) \in f^{-1}$ and $(f(a_2), a_2) \in f^{-1}$.

Since f^{-1} is a function and $f(a_1) = f(a_2)$, then $a_1 = a_2$.

Therefore, f is injective.

Conversely, we prove if f is injective, then f^{-1} is a function.
Suppose f is injective.
Let $(a, b_1) \in f^{-1}$ and $(a, b_2) \in f^{-1}$.
Since f^{-1} is an inverse of f, then $(b_1, a) \in f$ and $(b_2, a) \in f$, so $f(b_1) = a$ and $f(b_2) = a$.
Thus, $f(b_1) = a = f(b_2)$.
Since f is injective, then $b_1 = b_2$.
Therefore, f^{-1} is a function. □

Theorem 36. ***The inverse of an invertible map is unique.***
Let $f : A \to B$ be an invertible map.
Then the inverse map is unique.

Proof. Since $f : A \to B$ is an invertible map, then there exists a map that is an inverse of f.
Let $g : B \to A$ and $h : B \to A$ be inverse maps of f.
To prove the inverse map is unique, we must prove $g = h$.
Observe that the domain of g equals B which equals the domain of h and the codomain of g equals A which equals the codomain of h.
Let $x \in B$ be arbitrary.
Since $g : B \to A$ is a map, then $g(x) \in A$.
Since f is a relation, then $(g(x), x) \in f$.
Since h and f are inverses, then $(x, g(x)) \in h$, so $h(x) = g(x)$.
Therefore, $g = h$, as desired. □

Theorem 37. *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. $f \circ g = I_B$.

Proof. We prove if g is an inverse of f, then $g \circ f = I_A$ and $f \circ g = I_B$.
Since $f : A \to B$ and $g : B \to A$ are maps, then $g \circ f : A \to A$ and $f \circ g : B \to B$ are maps and $(g \circ f)(a) = g(f(a))$ for all $a \in A$ and $(f \circ g)(b) = f(g(b))$ for all $b \in B$.
Suppose g is an inverse of f.

We prove $g \circ f = I_A$.
Let I_A be the identity map on A.
Then $dom(g \circ f) = A = dom I_A$.
Let $a \in A$.
Since f is a function, then $(a, f(a)) \in f$.
Since g is an inverse of f, then $(f(a), a) \in g$, so $g(f(a)) = a$.
Observe that

$$\begin{aligned} (g \circ f)(a) &= g(f(a)) \\ &= a \\ &= I_A(a). \end{aligned}$$

Hence, $(g \circ f)(a) = I(a)$ for every $a \in A$.
Therefore, $g \circ f = I_A$.

We prove $f \circ g = I_B$.
Let I_B be the identity map on B.
Then $dom(f \circ g) = B = dom I_B$.
Let $b \in B$.
Since g is a function, then $(b, g(b)) \in g$.
Since f is an inverse of g, then $(g(b), b) \in f$, so $f(g(b)) = b$.
Observe that

$$\begin{aligned}(f \circ g)(b) &= f(g(b)) \\ &= b \\ &= I(b).\end{aligned}$$

Hence, $(f \circ g)(b) = I(b)$ for every $b \in B$.
Therefore, $f \circ g = I_B$. □

Proof. Conversely, we prove if $g \circ f = I_A$ and $f \circ g = I_B$, then g is an inverse of f.
Suppose $g \circ f = I_A$ and $f \circ g = I_B$.

Let $(a, b) \in f$.
Then $a \in A$ and $b \in B$ and $f(a) = b$.
Since $a \in A$, then $a = I_A(a) = (g \circ f)(a) = g(f(a)) = g(b)$, so $(b, a) \in g$.
Hence, if $(a, b) \in f$, then $(b, a) \in g$.

Let $(b, a) \in g$.
Then $b \in B$ and $a \in A$ and $g(b) = a$.
Since $b \in B$, then $b = I_B(b) = (f \circ g)(b) = f(g(b)) = f(a)$, so $(a, b) \in f$.
Hence, if $(b, a) \in g$, then $(a, b) \in f$.
Since $(b, a) \in g$ implies $(a, b) \in f$ and $(a, b) \in f$ implies $(b, a) \in g$, then $(b, a) \in g$ iff $(a, b) \in f$.
Therefore, g is an inverse of f. □

Corollary 38. *Let $f : A \to B$ be an invertible map. Then*
1. $f^{-1} \circ f = I_A$
2. $f \circ f^{-1} = I_B$.

Proof. Since $f : A \to B$ is an invertible map, then the inverse map $f^{-1} : B \to A$ exists, so f^{-1} is an inverse of f.
Therefore, $f^{-1} \circ f = I_A$ and $f \circ f^{-1} = I_B$. □

Theorem 39. ***An invertible map is bijective.***
Let $f : A \to B$ be a map.
Then f is invertible iff f is bijective.

Proof. We prove if f is bijective, then f is invertible.
Suppose f is bijective.
Then f is injective and surjective.
Since f is injective, then the inverse relation f^{-1} is a function.
Since f^{-1} is a relation, then $domf^{-1} = rngf$ and $rngf^{-1} = domf$.
Since f is surjective, then $rngf = B$.
Thus, $domf^{-1} = rngf = B$ and $rngf^{-1} = domf = A \subset A$.
Since f^{-1} is a function and $domf^{-1} = B$ and $rngf^{-1} \subset A$, then $f^{-1} : B \to A$ is a map.
Since f^{-1} is the inverse of f, then f is invertible. □

Proof. Conversely, we prove if f is invertible, then f is bijective.
Suppose f is invertible.
Then the inverse map $f^{-1} : B \to A$ exists.
Hence, the inverse relation f^{-1} is a function, so f is injective.

Let $b \in B$.
Since $f^{-1} : B \to A$ is a map, then $f^{-1}(b) \in A$.
Let $a = f^{-1}(b)$.
Then $a \in A$.
Since f^{-1} is the inverse of f and $f^{-1}(b) = a$, then $f(a) = b$.
Therefore, there exists $a \in A$ such that $f(a) = b$, so f is surjective.
Since f is injective and surjective, then f is bijective. □

Lemma 40. *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.

Proof. Suppose the map $f : A \to B$ is a bijection.
Then f is bijective, so f is invertible.
Hence, the map $f : A \to B$ is invertible, so the inverse map $f^{-1} : B \to A$ exists.

We prove f^{-1} is injective.
Let $b_1, b_2 \in B$ such that $f^{-1}(b_1) = f^{-1}(b_2)$.
Let $a = f^{-1}(b_1) = f^{-1}(b_2)$.
Then $f^{-1}(b_1) = a$ and $f^{-1}(b_2) = a$, so $(b_1, a) \in f^{-1}$ and $(b_2, a) \in f^{-1}$.
Since f^{-1} is the inverse of f, then $(a, b_1) \in f$ and $(a, b_2) \in f$.
Since f is a function and $(a, b_1) \in f$ and $(a, b_2) \in f$, then $b_1 = b_2$.
Therefore, f^{-1} is injective.

We prove f^{-1} is surjective.
Let $a \in A$.
Since $f : A \to B$ is a map, then $f(a) \in B$.
Let $b = f(a)$.
Then $b \in B$.
Since f^{-1} is the inverse of f and $f(a) = b$, then $f^{-1}(b) = a$.
Thus, there exists $b \in B$ such that $f^{-1}(b) = a$, so f^{-1} is surjective.

Since f^{-1} is injective and surjective, then f^{-1} is bijective.

Since $f^{-1} : B \to A$ is a map and f^{-1} is bijective, then $f^{-1} : B \to A$ is a bijection. □

Theorem 41. *Let $f : A \to B$ be a bijection. Then*

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

Proof. Since $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is a bijection, so $(f^{-1})^{-1} : A \to B$ is a bijection.

Observe that $(f^{-1})^{-1} : A \to B$ and $f : A \to B$ have the same domain A and same codomain B.

Let $a \in A$ be arbitrary.

Since f is a function, then there is a unique $b \in B$ such that $f(a) = b$.

Since f^{-1} is the inverse of f, then $f^{-1}(b) = a$.

Since $(f^{-1})^{-1}$ is the inverse of f^{-1}, then $(f^{-1})^{-1}(a) = b$.

Thus, $(f^{-1})^{-1}(a) = b = f(a)$.

Hence, $(f^{-1})^{-1}(a) = f(a)$ for all $a \in A$.

Therefore, $(f^{-1})^{-1} = f$. □

Theorem 42. *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. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. Since $f : A \to B$ and $g : B \to C$ are bijections, then the composition $g \circ f : A \to C$ is a bijection, so $(g \circ f)^{-1} : C \to A$ is a bijection.

Since $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is a bijection.

Since $g : B \to C$ is a bijection, then $g^{-1} : C \to B$ is a bijection.

Thus, the composition $f^{-1} \circ g^{-1} : C \to A$ is a bijection.

Observe that $(g \circ f)^{-1} : C \to A$ and $f^{-1} \circ g^{-1} : C \to A$ have the same domain C and same codomain A.

Let $c \in C$ be arbitrary.

Since $(g \circ f)^{-1}$ is a function, then there exists a unique $a \in A$ such that $(g \circ f)^{-1}(c) = a$.

Since $(g \circ f)^{-1}$ is the inverse of $g \circ f$, then $(g \circ f)(a) = c$.

Since f is a function and $a \in A$, then there exists a unique $b \in B$ such that $f(a) = b$.

Thus, $c = (g \circ f)(a) = g(f(a)) = g(b)$.

Since g^{-1} is the inverse of g and $g(b) = c$, then $g^{-1}(c) = b$.

Since f^{-1} is the inverse of f and $f(a) = b$, then $f^{-1}(b) = a$.

Observe that

$$\begin{aligned} (g \circ f)^{-1}(c) &= a \\ &= f^{-1}(b) \\ &= f^{-1}(g^{-1}(c)) \\ &= (f^{-1} \circ g^{-1})(c). \end{aligned}$$

Thus, $(g \circ f)^{-1}(c) = (f^{-1} \circ g^{-1})(c)$ for all $c \in C$.
Therefore, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

Image and inverse image of functions

Proposition 43. *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.*

Proof. We prove 1.
We prove if f is injective, then every $b \in B$ has at most one preimage.
Suppose f is injective.
Let $b \in B$.
Either there exists $a \in A$ such that $f(a) = b$ or there does not exist $a \in A$ such that $f(a) = b$.
We consider each case separately.
Case 1: Suppose there does not exist $a \in A$ such that $f(a) = b$.
Then b has no preimage.
Case 2: Suppose there exists $a \in A$ such that $f(a) = b$.
Then a is a pre-image of b, so b has at least one pre-image.
Suppose $a_1, a_2 \in A$ are pre-images of b.
Then $f(a_1) = b$ and $f(a_2) = b$, so $f(a_1) = f(a_2)$.
Since f is injective, then $a_1 = a_2$, so there is at most one pre-image of b.
In either case, at most one preimage of b exists. □

Proof. Conversely, we prove if every $b \in B$ has at most one preimage, then f is injective.
Suppose every $b \in B$ has at most one preimage.
To prove f is injective, let $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$.
Let $b = f(a_1) = f(a_2)$.
Since $f : A \to B$ is a map, then $b \in B$.
Hence, b has at most one preimage, so there is at most one $a \in A$ such that $f(a) = b$.
Therefore, $a_1 = a_2$. □

Proof. We prove 2.
We prove if f is surjective, then every $b \in B$ has at least one pre-image.
Suppose f is surjective.
Let $b \in B$ be arbitrary.
Since f is surjective, then there exists $a \in A$ such that $f(a) = b$.
Hence, a is a pre-image of b, so b has at least one pre-image. □

Proof. We prove 3.
We prove if f is bijective, then every $b \in B$ has exactly one pre-image.
Suppose f is bijective.
Then f is injective and surjective.

Let $b \in B$.
Since f is surjective, then b has at least one pre-image.
Since f is injective, then b has at most one pre-image.
Since b has at least one pre-image and b has at most one pre-image, then b has exactly one pre-image. □

Proposition 44. *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.

Proof. We prove 1.
We prove $f(\emptyset) = \emptyset$ by contradiction.
Suppose $f(\emptyset) \neq \emptyset$.
Then there exists $b \in f(\emptyset)$, so there exists $x \in \emptyset$ such that $f(x) = b$.
Since $\emptyset$ is empty, then $x \notin \emptyset$.
Thus, we have $x \in \emptyset$ and $x \notin \emptyset$, a contradiction.
Therefore, $f(\emptyset) = \emptyset$. □

Proof. We prove 2.
We prove $f^{-1}(\emptyset) = \emptyset$ by contradiction.
Suppose $f^{-1}(\emptyset) \neq \emptyset$.
Then there exists $x \in f^{-1}(\emptyset)$, so $x \in A$ and $f(x) \in \emptyset$.
Since $\emptyset$ is empty, then $f(x) \notin \emptyset$.
Thus, we have $f(x) \in \emptyset$ and $f(x) \notin \emptyset$, a contradiction.
Therefore, $f^{-1}(\emptyset) = \emptyset$. □

Proof. We prove 3.
We prove $f(A) = rngf$.
Since $b \in f(A)$ iff there exists $a \in A$ such that $f(a) = b$ iff $b \in rngf$, then $b \in f(A)$ iff $b \in rngf$.
Therefore, $f(A) = rngf$. □

Proof. We prove 4.
We prove $f^{-1}(B) = A$.
Since $f^{-1}(B) = \{x \in A : f(x) \in B\}$, then $f^{-1}(B) \subset A$.

Let $x \in A$.
Since $f : A \to B$ is a map, then $f(x) \in B$.
Since $x \in A$ and $f(x) \in B$, then $x \in f^{-1}(B)$.
Thus, $A \subset f^{-1}(B)$.
Since $f^{-1}(B) \subset A$ and $A \subset f^{-1}(B)$, then $f^{-1}(B) = A$. □

Proposition 45. *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.

Proof. We prove 1.
Let A and B be subsets of X such that $A \subset B$.
We must prove $f(A) \subset f(B)$.
Let $y \in f(A)$.
Then there exists $x \in A$ such that $f(x) = y$.
Since $x \in A$ and $A \subset B$, then $x \in B$.
Thus, there exists $x \in B$ such that $f(x) = y$, so $y \in f(B)$.
Therefore, $f(A) \subset f(B)$. □

Proof. We prove 2.
Let A and B be subsets of X.
We must prove $f(A \cup B) = f(A) \cup f(B)$.
Observe that

$$\begin{aligned} y \in f(A \cup B) &\Leftrightarrow \text{there exists } x \in A \cup B \text{ such that } y = f(x) \\ &\Leftrightarrow \text{either there exists } x \in A \text{ or there exists } x \in B \text{ and } y = f(x) \\ &\Leftrightarrow \text{either there exists } x \in A \text{ and } y = f(x) \text{ or there exists } x \in B \text{ and } y = f(x) \\ &\Leftrightarrow \text{either } y \in f(A) \text{ or } y \in f(B) \\ &\Leftrightarrow y \in f(A) \cup f(B). \end{aligned}$$

Therefore, $y \in f(A \cup B)$ iff $y \in f(A) \cup f(B)$, so $f(A \cup B) = f(A) \cup f(B)$. □

Proof. We prove 2.
Let A and B be subsets of X.
We first prove $f(A \cup B) \subset f(A) \cup f(B)$.
Let $y \in f(A \cup B)$.
Then there exists $x \in A \cup B$ such that $f(x) = y$.
Since $x \in A \cup B$, then either $x \in A$ or $x \in B$.
Case 1: Suppose $x \in A$.
Since $x \in A$ and $y = f(x)$, then $y \in f(A)$.
Case 2: Suppose $x \in B$.
Since $x \in B$ and $y = f(x)$, then $y \in f(B)$.
Thus, either $y \in f(A)$ or $y \in f(B)$, so $y \in f(A) \cup f(B)$.
Therefore, $f(A \cup B) \subset f(A) \cup f(B)$.

We next prove $f(A) \cup f(B) \subset f(A \cup B)$.
Let $y \in f(A) \cup f(B)$.
Then either $y \in f(A)$ or $y \in f(B)$.
Case 1: Suppose $y \in f(A)$.
Then there exists $a \in A$ such that $f(a) = y$.
Since $a \in A$, then either $a \in A$ or $a \in B$, so $a \in A \cup B$.
Since $a \in A \cup B$ and $f(a) = y$, then $y \in f(A \cup B)$.
Case 2: Suppose $y \in f(B)$.
Then there exists $b \in B$ such that $f(b) = y$.
Since $b \in B$, then either $b \in A$ or $b \in B$, so $b \in A \cup B$.
Since $b \in A \cup B$ and $f(b) = y$, then $y \in f(A \cup B)$.
Hence, in either case, $y \in f(A \cup B)$.
Therefore, $f(A) \cup f(B) \subset f(A \cup B)$.

Since $f(A \cup B) \subset f(A) \cup f(B)$ and $f(A) \cup f(B) \subset f(A \cup B)$, then $f(A \cup B) = f(A) \cup f(B)$. □

Proof. We prove 3.
Let A and B be subsets of X.
We prove $f(A \cap B) \subset f(A) \cap f(B)$.
Let $y \in f(A \cap B)$.
Then there exists $x \in A \cap B$ such that $f(x) = y$.
Since $x \in A \cap B$, then $x \in A$ and $x \in B$.
Since $x \in A$ and $f(x) = y$, then $y \in f(A)$.
Since $x \in B$ and $f(x) = y$, then $y \in f(B)$.
Thus, $y \in f(A)$ and $y \in f(B)$, so $y \in f(A) \cap f(B)$.
Therefore, $f(A \cap B) \subset f(A) \cap f(B)$. □

Proof. We prove 4.
We prove $f(A \cap B) = f(A) \cap f(B)$ for every subset A and B of X iff f is injective.

We first prove if f is injective, then $f(A \cap B) = f(A) \cap f(B)$ for every subset A and B of X.
Suppose f is injective.
Let A and B be subsets of X.
We prove $f(A) \cap f(B) \subset f(A \cap B)$.

Let $y \in f(A) \cap f(B)$.
Then $y \in f(A)$ and $y \in f(B)$.
Since $y \in f(A)$, then $y = f(a)$ for some $a \in A$.
Since $y \in f(B)$, then $y = f(b)$ for some $b \in B$.
Hence, $f(a) = y = f(b)$.
Since f is injective and $f(a) = f(b)$, then $a = b$.
Since $a = b$ and $b \in B$, then $a \in B$.
Since $a \in A$ and $a \in B$, then $a \in A \cap B$.

Since $a \in A \cap B$ and $f(a) = y$, then $y \in f(A \cap B)$.
Therefore, $f(A) \cap f(B) \subset f(A \cap B)$.
Since $f(A \cap B) \subset f(A) \cap f(B)$ and $f(A) \cap f(B) \subset f(A \cap B)$, then $f(A \cap B) = f(A) \cap f(B)$.

Conversely, we prove if $f(A \cap B) = f(A) \cap f(B)$ for every subset A and B of X, then f is injective.
We prove by contrapositive.
Suppose f is not injective.
Then there exist $x_1, x_2 \in X$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.
We must prove there exist subsets A and B of X such that $f(A \cap B) \neq f(A) \cap f(B)$.
Let $A = \{x_1\}$ and $B = \{x_2\}$.
Since $x_1 \in X$ and $A = \{x_1\}$, then $A \subset X$.
Since $x_2 \in X$ and $B = \{x_1\}$, then $B \subset X$.

We prove $f(A \cap B) \neq f(A) \cap f(B)$.
If $A \cap B \neq \emptyset$, then there exists x such that $x \in A \cap B$, so $x \in A$ and $x \in B$.
Hence, $x \in \{x_1\}$ and $x \in \{x_2\}$, so $x = x_1$ and $x = x_2$.
Thus, $x_1 = x = x_2$.
Therefore, if $A \cap B \neq \emptyset$, then $x_1 = x_2$, so if $x_1 \neq x_2$, then $A \cap B = \emptyset$.
Since $x_1 \neq x_2$, then we conclude $A \cap B = \emptyset$.
Since $x_1 \in A$, then $f(x_1) \in f(A)$.
Since $x_2 \in B$, then $f(x_2) \in f(B)$.
Since $f(x_1) = f(x_2)$ and $f(x_2) \in f(B)$, then $f(x_1) \in f(B)$.
Thus, $f(x_1) \in f(A)$ and $f(x_1) \in f(B)$, so $f(x_1) \in f(A) \cap f(B)$.
Hence, $f(A) \cap f(B) \neq \emptyset$.
Therefore, $f(A \cap B) = f(\emptyset) = \emptyset \neq f(A) \cap f(B)$, as desired. □

Proposition 46. *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.

Proof. We prove 1.
Let C and D be subsets of Y such that $C \subset D$.
Let $x \in f^{-1}(C)$.
Then $x \in X$ and $f(x) \in C$.
Since $f(x) \in C$ and $C \subset D$, then $f(x) \in D$.
Hence, $x \in X$ and $f(x) \in D$, so $x \in f^{-1}(D)$.
Therefore, $f^{-1}(C) \subset f^{-1}(D)$. □

Proof. We prove 2.

Let C and D be subsets of Y.

We must prove $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

Observe that

$$\begin{aligned}
x \in f^{-1}(C \cup D) &\Leftrightarrow x \in X \text{ and } f(x) \in C \cup D \\
&\Leftrightarrow x \in X \text{ and either } f(x) \in C \text{ or } f(x) \in D \\
&\Leftrightarrow \text{either } x \in X \text{ and } f(x) \in C \text{ or } x \in X \text{ and } f(x) \in D \\
&\Leftrightarrow \text{either } x \in f^{-1}(C) \text{ or } x \in f^{-1}(D) \\
&\Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D).
\end{aligned}$$

Therefore, $x \in f^{-1}(C \cup D)$ iff $x \in f^{-1}(C) \cup f^{-1}(D)$, so $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$. ☐

Proof. We prove 3.

Let C and D be subsets of Y.

We must prove $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

Observe that

$$\begin{aligned}
x \in f^{-1}(C \cap D) &\Leftrightarrow x \in X \text{ and } f(x) \in C \cap D \\
&\Leftrightarrow x \in X \text{ and } f(x) \in C \text{ and } f(x) \in D \\
&\Leftrightarrow x \in X \text{ and } f(x) \in C \text{ and } x \in X \text{ and } f(x) \in D \\
&\Leftrightarrow x \in f^{-1}(C) \text{ and } x \in f^{-1}(D) \\
&\Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D).
\end{aligned}$$

Therefore, $x \in f^{-1}(C \cap D)$ iff $x \in f^{-1}(C) \cap f^{-1}(D)$, so $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$. ☐

Proposition 47. ***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.

Proof. We prove 1.

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

Let $S \subset A$.

Suppose $x \in S$.

Then $f(x) \in f(S)$.

Since $x \in S$ and $S \subset A$, then $x \in A$.

Since $x \in A$ and $f(x) \in f(S)$, then $x \in f^{-1}(f(S))$.

Therefore, $S \subset f^{-1}(f(S))$. ☐

Proof. We prove 2.

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

We first prove if $f^{-1}(f(S)) = S$ for every subset S of A, then f is injective.
Suppose $f^{-1}(f(S)) = S$ for every subset S of A.
To prove f is injective, let $a, b \in A$ such that $f(a) = f(b)$.
We must prove $a = b$.
Let $S = \{a\}$.
Since $a \in A$, then $S \subset A$.
Hence, $f^{-1}(f(S)) = S$.
Since $a \in S$, then $f(a) \in f(S)$.
Since $f(b) = f(a)$, then $f(b) \in f(S)$.
Since $b \in A$ and $f(b) \in f(S)$, then $b \in f^{-1}(f(S))$.
Thus, $b \in S$, so $b \in \{a\}$.
Therefore, $b = a$, as desired.

Conversely, we prove if f is injective, then $f^{-1}(f(S)) = S$ for every subset S of A.
Suppose f is injective.
Let $S \subset A$.
We must prove $f^{-1}(f(S)) = S$.
Let $x \in f^{-1}(f(S))$.
Then $x \in A$ and $f(x) \in f(S)$.
Since $f(x) \in f(S)$, then there exists $s \in S$ such that $f(s) = f(x)$.
Since f is injective, then $s = x$.
Since $s \in S$, then $x \in S$.
Therefore, $f^{-1}(f(S)) \subset S$.
Since $f^{-1}(f(S)) \subset S$ and $S \subset f^{-1}(f(S))$, then $f^{-1}(f(S)) = S$. □

Proposition 48. ***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.

Proof. We prove 1.
Let $T \subset B$.
We prove $f(f^{-1}(T)) \subset T$.

Let $y \in f(f^{-1}(T))$.
Then there exists $x \in f^{-1}(T)$ such that $f(x) = y$.
Since $x \in f^{-1}(T)$, then $x \in A$ and $f(x) \in T$.
Thus, $y \in T$.
Therefore, $f(f^{-1}(T)) \subset T$. □

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

We first prove if f is surjective, then $f(f^{-1}(T)) = T$ for every subset T of B.
Suppose f is surjective.
Let $T \subset B$.
Let $y \in T$.
Since f is surjective, then there exists $x \in A$ such that $f(x) = y$.
Since $x \in A$ and $f(x) \in T$, then $x \in f^{-1}(T)$.
Since $y = f(x)$ and $x \in f^{-1}(T)$, then $y \in f(f^{-1}(T))$.
Therefore, $T \subset f(f^{-1}(T))$.
Since $f(f^{-1}(T)) \subset T$ and $T \subset f(f^{-1}(T))$, then $f(f^{-1}(T)) = T$.

Conversely, we prove if $f(f^{-1}(T)) = T$ for every subset T of B, then f is surjective.
Suppose $f(f^{-1}(T)) = T$ for every subset T of B.
Since $B \subset B$, then $f(f^{-1}(B)) = B$.
Observe that

$$\begin{aligned} B &= f(f^{-1}(B)) \\ &= f(A) \\ &= rngf. \end{aligned}$$

Therefore, $rngf = B$, so f is surjective, as desired. □