Definitions

Definition 1 (Subset)**.** Set A is a subset of a set B (written $A \subseteq B$) if $a \in A \implies a \in B$.

Definition 2 (Equality of sets)**.** Sets A and B are equal (written $A = B$) if $A \subseteq B \wedge B \subseteq A$.

Definition 3 (Proper subset)**.** Set A is a proper subset of B (written $A \subset B$) if $A \subseteq B \wedge A \neq B$

Definition 4 (Empty set)**.** Emptyset ($\varnothing$) is defined as a set containing no elements: $\forall x : x \notin \varnothing$.

Definition 5 (Union of sets)**.** Union of sets A and B is a set $A \cup B = \{x : x \in A \vee x \in B\}$.

Definition 6 (Intersection of sets)**.** Intersection of sets A and B is a set $A \cap B = \{x : x \in A \wedge x \in B\}$.

Definition 7 (Disjoint sets)**.** Sets A and B are disjoint if $A \cap B = \varnothing$.

Definition 8 (Set compliment)**.** Let U be the universal class, and let $A \subset U$. The compliment of A is the set $A' = \{x \in U : x \notin A\}$.

Definition 9 (Set difference)**.** The difference of sets A and B is the set $A \setminus B = A \cap B' = \{x \in A : x \notin B\}$.

Definition 10 (Cartesian product of sets)**.** Cartesian product of sets A and B is the set $A \times B = \{(a, b) : a \in A \wedge b \in B\}$.

Definition 11 (Binary Relation)**.** Relation R is a binary relation between sets A and B if $R \subseteq A \times B$.

The notation xRy means $(x, y) \in R$. Let $R \subseteq A \times B$. The set A is called the domain of R, and the set B is the co–domain of R.

Definition 12 (Endorelation)**.** Relation R is an endorelation on set A if $R \subseteq A^2 = A \times A$.

Definition 13 (Image of a set under a binary relation)**.** Let $R \subseteq A \times B$ be a binary relation. Then the image of A under R is the set $Im(R) = \{y \in B : \exists x \in A : xRy\}$.

Definition 14 (Preimage of a set under binary relation)**.** Let $R \subseteq A \times B$ be a binary relation, and let $Y \subseteq B$. Then the preimage of Y under R (written $R^{-1}(Y)$) is $R^{-1}(Y) = \{x \in A : \exists y \in Y : xRy\}$.

Definition 15 (Field of a binary relation)**.** Let R be a binary relation. Then $Field(R) = Dom(R) \cup Im(R)$.

Definition 16 (Injection)**.** A binary relation $R \subseteq A \times B$ is injective if $\forall x, z \in A, \forall y \in B : xRy \wedge zRy \implies x = z$.

In example, the relation $R = \{(x, x^2)\} \subseteq \mathbb{Z} \times \mathbb{Z}$ is not injective, since both $(2, 4)$ and $(-2, 4)$ are in R, and hence injectivity does not hold.

Definition 17 (Surjection)**.** A binary relation $R \subseteq A \times B$ is surjective if $\forall y \in B\ \exists x \in A : xRy$.

In example, the relation $R = \{(x, x^2)\} \subseteq \mathbb{Z} \times \mathbb{Z}$ is not surjective, since no preimage exists for $3 \in \mathbb{Z}$, since $\sqrt{3} \notin \mathbb{Z}$.

Definition 18 (Bijection)**.** Injective and surjective binary relation is called bijective.

Definition 19 (Set cardinality)**.** Cardinality of a set A, denoted as $|A|$, is a measure of the number of elements in the set.
$|A| = |B|$ if there exists a bijection $f : A \to B$.
$|A| \leqslant |B|$ if there exists an injection $f : A \to B$.
$|A| < |B|$ if there exists an injection $f : A \to B$, but no bijection $g : A \to B$ exists.

Definition 20 (Countable set)**.** Set A is countable if $|A| = |B|$, where $B \subseteq \mathbb{N}$.

Definition 21 (Countably infinite set)**.** Set A is countably infinite if there exists a bijection $f : A \to \mathbb{N}$.

Definition 22 (Reflexivity)**.** Binary relation R on a set A is **reflexive** if every element x in A is related to itself: $\forall x \in A : xRx$.

In example, relation $\leqslant$ on $\mathbb{Z}$ is reflexive, since $\forall a \in \mathbb{Z} : a \leqslant a$. However, the relation $<$ is not reflexive, since $a < a$ does not hold.

Definition 23 (Anti–reflexivity)**.** Binary relation R is called **anti–reflexive** if every element x in A is not related to itself: $\forall x \in A : \neg(xRx)$.

In example, relation $<$ on $\mathbb{Z}$ is anti–reflexive, since $\forall a \in \mathbb{Z} : a \not< a$.

Definition 24 (Symmetry)**.** Relation R on a set A is called **symmetric** if $\forall x, y \in A : xRy \implies yRx$.

In example, equality relation $=$ on $\mathbb{R}$ is symmetric, since $\forall a, b \in \mathbb{R} : a = b \implies b = a$.

Definition 25 (Anti–symmetry)**.** Relation R on a set A is **anti–symmetric** if $\forall x, y \in A : xRy \wedge yRx \implies x = y$.

In example, relation $\leqslant$ is anti–symmetric, since $x \leqslant y \wedge y \leqslant x \implies x = y$.

Definition 26 (Asymmetry)**.** Relation R on a set A is **asymmetric** if $\forall x, y \in A : xRy \implies \neg(yRx)$.

In example: relation $<$ on $\mathbb{R}$ is asymmetric, since $x < y \implies \neg(y < x)$.

Definition 27 (Transitivity)**.** Relation R on a set A is **transitive** if $\forall x, y, z \in A : xRy \wedge yRz \implies xRz$.

In example, it can be seen that relations $<$ and $=$ are transitive

$$a < b \wedge b < c \implies a < c\ ,$$
$$a = b \wedge b = c \implies a = c\ .$$

Definition 28 (Connexity)**.** Relation R on a set A is **connex** if $\forall x, y \in A : xRy \vee yRx$.

Definition 29 (Trichotomy)**.** R is called **trichotomous** if $\forall x, y \in A : xRy \vee yRx \vee x = y$.

Definition 30 (Left–total binary relation)**.** A binary relation $R \subseteq A \times B$ is left–total if $\forall x \in A \; \exists y \in B : xRy$.

Definition 31 (Partial function)**.** A binary relation $R \subseteq A \times B$ is a partial function if $\forall x \in A, \forall y, z \in B : xRy \wedge xRz \implies y = z$.

In example, mapping $f : \mathbb{Z} \to \mathbb{Z}$ defined by $y = \sqrt{x}$ is not a partial function, since $2 = \sqrt{4} = -2$.

Definition 32 (Function, Mapping)**.** A binary relation $R \subseteq A \times B$ is a function (or a mapping) $F : A \to B$ if it is left-total, injective, and is a partial function.

The notation $a \overset{f}{\mapsto} b$ means that element $a \in A$ is mapped to element $b \in B$ by mapping $f : A \to B$. Equivalently, the same can be expressed as $f(a) = b$. In other words, mapping $F : A \to B$ maps every element $a \in A$ to a *unique* element $b \in B$.

Definition 33 (Linear Map)**.** A **linear mapping** or **linear transformation** is a map $\mathbb{R}^n \to \mathbb{R}^m$ given by a matrix.

In example, given a 2×2 matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; ,$$

we can define a map $T_A : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$\forall (x, y) \in \mathbb{R}^2 : T_A(x, y) = (ax + by, cx + dy) \; .$$

This is actually matrix multiplication, that is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} \; .$$

Definition 34 (Permutation)**.** For any set S, a bijective mapping $\pi : S \to S$ is called a **permutation**.

Suppose $S = \{1, 2, 3\}$. Define a map $\pi : S \to S$ by

$$\begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \; .$$

It is easy to verify that this map is bijective, hence this map is a permutation of S.

Definition 35 (Identity Map)**.** The **identity map** id_S is such that $\forall s \in S : s \mapsto s$.

In example, for $S = \{1, 2, 3\}$, the identity map id_S is

$$\begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \; .$$

Definition 36 (Function Composition)**.** A **composition of function** $f : A \to B$ and $g : B \to C$ is a new function $h : A \to C$ defined by

$$(g \circ f)(x) = g(f(x)) \ .$$

Note that $g(f(x)) = (g \circ f)(x) \neq (f \circ g)(x) = f(g(x))$.

For example, consider the following sets

$$A = \{1, 2, 3\} \qquad B = \{a, b, c\} \qquad C = \{x, y, z\} \ .$$

Consider maps

$$f : A \to B \text{ defined by } \{1 \mapsto b, 2 \mapsto c, 3 \mapsto a\} \ ,$$
$$g : B \to C \text{ defined by } \{a \mapsto z, b \mapsto z, c \mapsto x\} \ .$$

The composition $g \circ f : A \to C$ is defined by $\{1 \mapsto z, 2 \mapsto x, 3 \mapsto z\}$.

It can be seen than the composition $f \circ g$ is not a valid map.

Definition 37 (Inverse Map)**.** Let $f : A \to B$ be a function. The **inverse map** $f^{-1} : B \to A$ is a function such that

$$f \circ f^{-1} = id_B \ ,$$
$$f^{-1} \circ f = id_A \ .$$

Function $f : \mathbb{R}^+ \to \mathbb{R}$ defined by $f(x) = \ln(x)$ has an inverse $f^{-1}(x) = e^x$.

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = f(e^x) = \ln e^x = x \ ,$$
$$(f^{-1} \circ f)(x) = f^{-1}(\ln x) = e^{\ln x} = x \ .$$

Definition 38 (Equivalence Relation)**.** A binary relation R on a set X is an equivalence relation iff it is reflexive, symmetric and transitive.

Definition 39 (Set partition)**.** A partition of a set X is a set of non-empty subsets $A_i \subset X$ such that they are pairwise disjoint $A_i \cap A_j = \emptyset \forall i \neq j$, and $\bigcup_i A_i = X$.

Any such subset A_i is an equivalence class under equivalence relation $\sim$. Every equivalence relation gives rise to a partition, and likewise if there exists a partition of some set, there exists an equivalence relation which generates this partition.

Definition 40 (Equivalence Class)**.** An equivalence class of $x \in X$ under equivalence relation R, denoted as $[x]$ is a set of elements that are equivalent under R : $[x] = \{y \in X : x \sim y\}$.

Definition 41 (Factor Set)**.** The factor set of a set X under equivalence relation $\sim$, denoted as $X/\sim$, is a set consisting of representative of each of the equivalence classes in a partition. The cardinality of the factor set is equal to the number of equivalence classes in a partition generated by $\sim$.

Definition 42 (Setoid)**.** A set with an equivalence relation on it is called a setoid.

Definition 43 (Partial Order)**.** A (weak) partial order on a set X is reflexive, anti–symmetric and transitive binary relation on X.

Definition 44 (Strict partial order)**.** A strict partial order on a set X is anti–reflexive, asymmetric (and hence also anti–symmetric) and transitive relation on X.

Definition 45 (Partially Ordered Set)**.** A set X with a partial order relation R on it, denoted as (X, R) is a partially ordered set, or a poset.

Definition 46 (Comparable Elements)**.** Let X be a set partially ordered by R. $a, b \in X$ are comparable if $aRb \vee bRa$ is true, otherwise they are incomparable.

Definition 47 (Interval on a Partially Ordered Set)**.** Let X be a set partially ordered by relations $\leqslant$ and $<$. The following intervals can be defined on X for all $a, b \in X$:

$$[a, b] = \{x \in X : a \leqslant x \leqslant b\} \qquad (a, b) = \{x \in X : a < x < b\}$$
$$(a, b] = \{x \in X : a < x \leqslant b\} \qquad [a, b) = \{x \in X : a \leqslant x < b\}$$

Definition 48 (Total Order, Linear Order, Chain)**.** A total order (also, linear order, a chain) is a connex partial order – a binary relation that is reflexive, anti–symmetric, transitive, and connex.

Definition 49 (Strict total order)**.** A strict total order is a strict connex partial order.

Definition 50 (Totally Ordered Set)**.** A totally ordered (also, linearly ordered) set is a set equipped with a total order relation.

Definition 51 (Minimal Element of a Poset)**.** Let P be a set partially ordered by R, and let $S \subseteq P$. Element $m \in S$ is a minimal element of S if $\forall x \in S : xRm \implies x = m$.

Definition 52 (Maximal Element of a Poset)**.** Let P be a set partially ordered by R, and let $S \subseteq P$. Element $m \in S$ is a maximal element of S if $\forall x \in S : mRx \implies x = m$.

Definition 53 (Least Element of a Poset)**.** Let P be a set partially ordered by R, and let $S \subseteq P$. Element $l \in S$ is the least element of S if $\forall x \in S : lRx$.

Definition 54 (Greatest Element of a Poset)**.** Let P be a set partially ordered by R, and let $S \subseteq P$. Element $g \in S$ is the greatest element of S if $\forall x \in S : xRg$.

Definition 55 (Minimum in a Totally Ordered Set)**.** In case of a total order, the notions of minimal and least elements coincide, and such element is called minimum element.

Definition 56 (Maximum in a Totally Ordered Set)**.** In case of a total order, the notions of maximal and greatest elements coincide, and such element is called maximum element.

Corollary 1. A finite chain always has a greatest and a least element.

Definition 57 (Upper Bound of a Partially Ordered Set)**.** Let P be a set partially ordered by R. Let $S \subseteq P$. Element $\lambda \in P$ is an upper bound of S if $\forall x \in S : xR\lambda$.

Definition 58 (Lower Bound of a Partially Ordered Set)**.** Let P be a set partially ordered by R. Let $S \subseteq P$. Element $\lambda \in P$ is a lower bound of S if $\forall x \in S : \lambda R x$.

Definition 59 (Supremum of a partially ordered set)**.** Let P be a set partially ordered by R. Let $S \subseteq P$. An upper bound I of S is a supremum (denoted as $\sup S$) if I is the least upper bound: $\forall U \in P : IRU$.

Definition 60 (Infimum of a partially ordered set)**.** Let P be a set partially ordered by R. Let $S \subseteq P$. A lower bound I of S is an infimum (denoted as $\inf S$) if I is the greatest lower bound: $\forall U \in P : URI$.

Definition 61 (Lattice)**.** A lattice $(L, \wedge, \vee)$ is a partially ordered set in which every two elements have a supremum and an infimum. It can be seen that a lattice is both meet– and join–semilattice.

Definition 62 (Bounded Lattice)**.** A bounded lattice is an algebraic structure $(L, \vee, \wedge, 0, 1)$ such that

- $(L, \vee, \wedge)$ is a lattice
- 0 (the lattice's bottom ($\bot$)) is an identity element for the join ($\vee$) operation: $\forall a \in L : a \vee 0 = a$.
- 1 (the lattice's top ($\top$)) is an identity element for the meet ($\wedge$) operation: $\forall a \in L : a \wedge 1 = a$.

Definition 63 (Complemented Lattice)**.** A complemented lattice $(L, \wedge, \vee)$ is a lattice in which every element $a \in L$ has a complement – an element $\neg a \in L$ satisfying $a \vee \neg a = 1$ and $a \wedge \neg a = 0$.

Definition 64 (Distributive Lattice)**.** A lattice $(L, \wedge, \vee)$ is distributive if $\forall x, y, z \in L : x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

Definition 65 (Boolean algebra, Boolean lattice)**.** A Boolean algebra $(L, \wedge, \vee, \neg, 0, 1)$ is a complemented distributive lattice.

A Boolean algebra gives rise to a Boolean ring, and vice versa.