Introduction to Set Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

1. Relations, Functions and Orderings
   - Ordered Pairs
   - Relations
   - Functions
   - Equivalences and Partitions
   - Orderings

Subsection 1

Ordered Pairs

Unordered versus Ordered Pairs

- We show how various mathematical concepts, such as relations, functions, and orderings can be represented by sets.
- We begin by introducing the notion of an ordered pair.
- If a and b are sets, then the unordered pair $\{a, b\}$ is a set whose elements are exactly a and b. The "order" in which a and b are put together plays no role, i.e., $\{a, b\} = \{b, a\}$.
- Sometimes, we need to pair a and b so that it is possible to "decipher" which set comes "first" and which comes "second."
- We denote this ordered pair of a and b by (a, b); a is the first coordinate of the pair (a, b), b is the second coordinate.
- The ordered pair has to be a set and it should be defined in such a way that two ordered pairs are equal if and only if their first coordinates are equal and their second coordinates are equal.
- There are many ways to define (a, b) so that these conditions are satisfied. We choose one (among many possible) definition.

Ordered Pairs and Equality

Definition (Ordered Pair)

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

- If $a \neq b$, (a, b) has two elements, $\{a\}$ and $\{a, b\}$.
  - We find the first coordinate by looking at the element of $\{a\}$.
  - The second coordinate is then the other element of $\{a, b\}$.
- If $a = b$, then $(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}\}$ has only one element.

Theorem

$(a, b) = (a', b')$ if and only if $a = a'$ and $b = b'$.

- If $a = a'$ and $b = b'$, then $(a, b) = \{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\} = (a', b')$.
- Assume, conversely, that $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$.
  - If $a \neq b$, $\{a\} = \{a'\}$ and $\{a, b\} = \{a', b'\}$. So, first, $a = a'$ and then $\{a, b\} = \{a, b'\}$ implies $b = b'$.
  - If $a = b$, $\{\{a\}, \{a, a\}\} = \{\{a\}\}$. So $\{a\} = \{a'\}$, $\{a\} = \{a', b'\}$, and we get $a = a' = b'$, so $a = a'$ and $b = b'$ holds in this case, too.

Ordered Triples, Quadruples, etc.

- With ordered pairs at our disposal, we can define
  - **ordered triples**
    $$(a, b, c) = ((a, b), c),$$
  - **ordered quadruples**
    $$(a, b, c, d) = ((a, b, c), d)$$
  - and so on.
- Also, we define ordered "**one-tuples**"
  $$(a) = a.$$
- The general definition of ordered n-tuples has to be postponed until natural numbers have been defined.

Subsection 2

Relations

Idea Behind Binary Relations

- Relations between objects of two sorts are called binary relations.
- Example:
  - A line ℓ is in relation R_1 with a point P if ℓ passes through P. Then R_1 is a binary relation between objects called lines and objects called points.
  - A positive integer m is in relation R_2 with a positive integer n if m divides n (without remainder).
  - Consider the relation R_1' between lines and points such that a line ℓ is in relation R_1' with a point P if P lies on ℓ. Obviously, a line ℓ is in relation R_1' to a point P exactly when ℓ is in relation R_1 to P. Although different properties were used to describe R_1 and R_1', we would ordinarily consider R_1 and R_1' to be one and the same relation, i.e., $R_1 = R_1'$.
  - Similarly, let a positive integer m be in relation R_2' with a positive integer n if n is a multiple of m. Again, the same ordered pairs (m, n) are related in R_2 as in R_2', and we consider R_2 and R_2' to be the same relation.

Binary Relations

Definition (Binary Relation)

A set R is a **binary relation** if all elements of R are ordered pairs, i.e., if for any $z \in R$, there exist x and y such that $z = (x, y)$.

- Example: The relation R_2 is simply the set

$$\{z : \text{ there exist positive integers } m \text{ and } n, \text{ such that } z = (m, n) \text{ and } m \text{ divides } n\}.$$

  Elements of R_2 are ordered pairs

$$\begin{array}{l} (1,1),(1,2),(1,3),\ldots \\ (2,2),(2,4),(2,6),\ldots, \\ (3,3),(3,6),(3,9),\ldots \\ \ldots \end{array}$$

- It is customary to write $x \; R \; y$ instead of $(x, y) \in R$. We say that x **is in relation** R **with** y if $x \; R \; y$ holds.

Domain and Range of a Relation

Definition

Let R be a binary relation.

(a) The set of all x which are in relation R with some y is called the **domain** of R and denoted by $\text{dom}R$.

$$\text{dom}R = \{x : \text{there exists } y \text{ such that } x\ R\ y\}.$$

$\text{dom}R$ is the set of all first coordinates of ordered pairs in R.

(b) The set of all y such that, for some x, x is in relation R with y is called the **range** of R, denoted by $\text{ran}R$.

$$\text{ran}R = \{y : \text{there exists } x \text{ such that } x\ R\ y\}.$$

$\text{ran}R$ is the set of all second coordinates of ordered pairs in R.
Both $\text{dom}R$ and $\text{ran}R$ exist for any relation R.

(c) The set $\text{dom}R \cup \text{ran}R$ is called the **field** of R and is denoted by $\text{field}R$.

(d) If $\text{field}R \subseteq X$, we say that R is a **relation in** X or that R is a **relation between elements of** X.

Illustrating the Terminology

- Example: Let R_2 be the previously defined relation: A positive integer m is in relation R_2 with a positive integer n if m divides n (without remainder).

$$\begin{aligned} \mathrm{dom} R_2 &= \{m : \text{there exists } n \text{ such that } m \text{ divides } n\} \\ &= \text{the set of all positive integers} \end{aligned}$$

because each positive integer m divides some n, e.g., $n = m$.

$$\begin{aligned} \mathrm{ran} R_2 &= \{n : \text{there exists } m \text{ such that } m \text{ divides } n\} \\ &= \text{the set of all positive integers} \end{aligned}$$

because each positive integer n is divided by some m, e.g., by $m = n$.
$\mathrm{field} R_2 = \mathrm{dom} R_2 \cup \mathrm{ran} R_2 =$ the set of all positive integers;
R_2 is a relation between positive integers.

Image and Inverse Image

Definition (Image and Inverse Image)

(a) The **image of** A **under** R, denoted $R[A]$, is the set of all y from the range of R related in R to some element of A.

$$R[A] = \{y \in \text{ran}R : \text{there exists } x \in A \text{ for which } x \; R \; y\}.$$

(b) The **inverse image of** B **under** R, denoted $R^{-1}[B]$, is the set of all x from the domain of R related in R to some element of B.

$$R^{-1}[B] = \{x \in \text{dom}R : \text{there exists } y \in B \text{ for which } x \; R \; y\}.$$

- Example:

$$\begin{aligned} R_2^{-1}[\{3,8,9,12\}] &= \{1,2,3,4,6,8,9,12\}; \\ R_2[\{2\}] &= \text{the set of all even positive integers.} \end{aligned}$$

Inverse of a Binary Relation

Definition (Inverse Realtion)

Let R be a binary relation. The inverse of R is the set

$$R^{-1} = \{z : z = (x, y) \text{ for some } x \text{ and } y \text{ such that } (y, x) \in R\}.$$

- Example: Again let

$$R_2 = \{z : z = (m, n),\ m \text{ and } n \text{ are positive integers, and } m \text{ divides } n\}.$$

Then

$$\begin{aligned} R_2^{-1} &= \{w : w = (n, m), \text{ and } (m, n) \in R_2\} \\ &= \{w : w = (n, m),\ m \text{ and } n \text{ are positive integers, and } m \text{ divides } n\}. \end{aligned}$$

In our description of R_2, we use variable m for the first coordinate and variable n for the second coordinate; we also state the property describing R_2 so that the variable m is mentioned first.

Example (Cont'd)

- It is a customary (though not necessary) practice to describe R_2^{-1} in the same way. All we have to do is use letter m instead of n, letter n instead of m and change the wording:

$$\begin{aligned} R_2^{-1} &= \{w : w = (m,n),\ n,\ m \text{ are positive integers, and } n \text{ divides } m\} \\ &= \{w : w = (m,n),\ m,\ n \text{ are positive integers, and } m \text{ is a multiple of } n\}. \end{aligned}$$

  Now R_2 and R_2^{-1} are described in a parallel way. In this sense, the inverse of the relation "divides" is the relation "is a multiple."

- Note that the symbol $R^{-1}[B]$ for the inverse image of B under R now also denotes the image of B under R^{-1}. Fortunately, these two sets are equal!

Inverse Image Under R versus Image Under R^{-1}

Lemma

The inverse image of B under R is equal to the image of B under R^{-1}.

- Notice first that $\text{dom}R = \text{ran}R^{-1}$. Now, $x \in \text{dom}R$ belongs to the inverse image of B under R if and only if, for some y, $(x, y) \in R$. But $(x, y) \in R$ if and only if $(y, x) \in R^{-1}$. Therefore, x belongs to the inverse image of B under R if and only if for some $y \in B$, $(y, x) \in R^{-1}$, i.e., if and only if x belongs to the image of B under R^{-1}.
- To simplify our notation we write $\{(x, y) : \mathbf{P}(x, y)\}$ instead of $\{w : w = (x, y)$ for some x and y such that $\mathbf{P}(x, y)\}$.
- Example: The inverse of R could be described in this notation $\{(x, y) : (y, x) \in R\}$. Recall that use of such notation is admissible only if we prove that there exists a set A such that, for all x and y, $\mathbf{P}(x, y)$ implies $(x, y) \in A$.

Composition of Binary Relations

Definition (Composition)

Let R and S be binary relations. The **composition of R and S** is the relation

$$S \circ R = \{(x,z) : \text{there exists } y \text{ for which } (x,y) \in R \text{ and } (y,z) \in S\}.$$

- So $(x,z) \in S \circ R$ means that for some y, $x \ R \ y$ and $y \ S \ z$.
- To find objects related to x in $S \circ R$,
  - we first find objects y related to x in R,
  - and then objects related to those y in S.
- Notice that R is performed first and S second, but the notation $S \circ R$ is customary (at least in the case of functions).

Special Relations

- Several types of relations are of special interest.

Definition (Membership and Identity Relations)

- The **membership relation on** A is defined by
$$\in_A = \{(a,b) : a \in A,\ b \in A, \text{ and } a \in b\}.$$
- The **identity relation on** A is defined by
$$\mathrm{Id}_A = \{(a,b) : a \in A,\ b \in A, \text{ and } a = b\}.$$

Definition (Cartesian Product)

Let A and B be sets. The set of all ordered pairs whose first coordinate is from A and whose second coordinate is from B is called the **cartesian product of** A **and** B and denoted $A \times B$. In other words,
$$A \times B = \{(a,b) : a \in A \text{ and } b \in B\}.$$

- Thus $A \times B$ is a relation in which every element of A is related to every element of B.

Existence of Cartesian Products

- To show that the set $A \times B$ exists:
  - First show that, if $a \in A$ and $b \in B$, then $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$.
  - Then conclude that

    $$A \times B = \{(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B)) : a \in A \text{ and } b \in B\}.$$

    Since $\mathcal{P}(\mathcal{P}(A \cup B))$ was proved to exist, the existence of $A \times B$ follows from the Axiom Schema of Comprehension.
- To be completely explicit, we can write,

  $$A \times B = \{w \in \mathcal{P}(\mathcal{P}(A \cup B)) : w = (a, b) \text{ for some } a \in A \text{ and } b \in B\}.$$
- We denote $A \times A$ by A^2.
- The cartesian product of three sets can be introduced readily: $A \times B \times C = (A \times B) \times C$. Notice that

  $$A \times B \times C = \{(a, b, c) : a \in A, b \in B \text{ and } c \in C\}$$

  (using an obvious extension of our notational convention).
- $A \times A \times A$ is usually denoted A^3.

Ternary Relations

Definition (Ternary Relation)

A **ternary relation** is a set of unordered triples. More explicitly, S is a ternary relation if for every $u \in S$, there exist x, y and z, such that $u = (x, y, z)$. If $S \subseteq A^3$, we say that S is a **ternary relation in** A. (Note that a binary relation R is in A if and only if $R \subseteq A^2$.)

- We could extend the concepts of this section to ternary relations and also define 4-ary or 17-ary relations.
- When natural numbers have been introduced, we will define n-ary relations in general.
- For technical reasons, a **unary relation** is any set. A **unary relation in** A is any subset of A.

  This agrees both with the idea that a unary relation in A should be a set of 1-tuples of elements of A and with the definition of $(x) = x$ adopted previously.

Subsection 3

Functions

Functions

- A function is a procedure or rule assigning to any object a from its domain a unique object b, the value of the function at a.
- A function is a special type of relation in which every object a from the domain is related to precisely one object in the range, the value of the function at a.

Definition (Function)

A binary relation F is called a **function** (or **mapping**, **correspondence**) if

$$a\ F\ b_1 \text{ and } a\ F\ b_2 \text{ imply } b_1 = b_2$$

for all a, b_1, b_2. I.e., a binary relation F is a function if and only if for every a from $\text{dom}F$ there is exactly one b such that $a\ F\ b$. This unique b is called the **value of** F **at** a and is denoted $F(a)$ or F_a. ($F(a)$ is not defined if $a \notin \text{dom}F$.) If F is a function with $\text{dom}F = A$ and $\text{ran}F \subseteq B$, it is customary to use the notations $F : A \to B$, $\langle F(a) : a \in A\rangle$, $\langle F_a : a \in A\rangle$, or $\langle F_a\rangle_{a\in A}$, for the function F. The range of the function F can then be denoted $\{F(a) : a \in A\}$ or $\{F_a\}_{a\in A}$.

Some Definitions Related to Functions

Lemma

Let F and G be functions. $F = G$ if and only if $\mathrm{dom}F = \mathrm{dom}G$ and $F(x) = G(x)$, for all $x \in \mathrm{dom}F$.

- Since functions are binary relations, the concepts of domain, range, image, inverse image, inverse, and composition are applicable.
- Here are some additional definitions:

Definition

Let F be a function and A and B sets.

(a) F is a **function on** A if $\mathrm{dom}F = A$.

(b) F is a **function into** B if $\mathrm{ran}F \subseteq B$.

(c) F is a **function onto** B if $\mathrm{ran}F = B$.

(d) The **restriction of the function** F **to** A is the function $F \upharpoonright A = \{(a, b) \in F : a \in A\}$. If G is a restriction of F to some A, we say that F is an **extension of** G.

Example

- Let $F = \{(x, \frac{1}{x^2}) : x \neq 0, x \text{ is a real number}\}$. F is a function:

  If $a\ F\ b_1$ and $a\ F\ b_2$, $b_1 = \frac{1}{a^2}$ and $b_2 = \frac{1}{a^2}$, so $b_1 = b_2$.

  Sometimes, we write $F = \langle \frac{1}{x^2} : x \text{ is a real number}, x \neq 0 \rangle$. The value of F at x, $F(x)$, equals $\frac{1}{x^2}$. F is function on A, where $A = \{x : x \text{ is a real number and } x \neq 0\}$. F is a function into the set of all real numbers, but not onto the set of all real numbers. If $B = \{x : x \text{ is a real number and } x > 0\}$, then F is onto B. If $C = \{x : 0 < x \leq 1\}$, then $f[C] = \{x : x \geq 1\}$ and $F^{-1}[C] = \{x : x \leq -1 \text{ or } x \geq 1\}$.

  The composition $f \circ f$ can be determined:

$$\begin{aligned} f \circ f &= \{(x, z) : \text{there is } y \text{ for which } (x, y) \in f \text{ and } (y, z) \in f\} \\ &= \{(x, z) : \text{there is } y \text{ for which } x \neq 0, \\ &\qquad\qquad y = \tfrac{1}{x^2}, \text{ and } y \neq 0,\ z = \tfrac{1}{y^2}\} \\ &= \{(x, z) : x \neq 0 \text{ and } z = x^4\}. \end{aligned}$$

  Notice that $f \circ f$ is a function.

Composition of Functions

Theorem

Let f and g be functions. Then $g \circ f$ is a function. $g \circ f$ is defined at x if and only if f is defined at x and g is defined at $f(x)$: $\text{dom}(g \circ f) = \text{dom} f \cap f^{-1}[\text{dom} g]$. Also, $(g \circ f)(x) = g(f(x))$, for all $x \in \text{dom}(g \circ f)$.

- We prove, first, that $g \circ f$ is a function. If $x(g \circ f)z_1$ and $x(g \circ f)z_2$, there exist y_1 and y_2 such that $x \ f \ y_1$, $y_1 \ g \ z_1$, and $x \ f \ y_2$, $y_2 \ g \ z_2$. Since f is a function, $y_1 = y_2$. So we get $y_1 \ g \ z_1$, $y_1 \ g \ z_2$, and, since g is also a function, $z_1 = z_2$.
- For the domain of $g \circ f$: $x \in \text{dom}(g \circ f)$ if and only if there is some z such that $x(g \circ f)z$, i.e., if and only if there is some z and some y such that $x \ f \ y$ and $y \ g \ z$. But this happens if and only if $x \in \text{dom} f$ and $y = f(x) \in \text{dom} g$. The last statement can be equivalently expressed as $x \in \text{dom} f$ and $x \in f^{-1}[\text{dom} g]$.

Composition and Invertibility

- This theorem is used in calculus to find domains of compositions of functions.
- Example: Let $f = \langle x^2 - 1 : x \text{ real}\rangle$, $g = \langle \sqrt{x} : x \geq 0\rangle$. Find the composition $g \circ f$.
  We determine the domain of $g \circ f$ first. $\text{dom} f$ is the set of all real numbers and $\text{dom} g = \{x : x \geq 0\}$. We find $f^{-1}[\text{dom} g] = \{x : f(x) \in \text{dom} g\} = \{x : x^2 - 1 \geq 0\} = \{x : x \geq 1 \text{ or } x \leq -1\}$. Therefore, $\text{dom}(g \circ f) = (\text{dom} f) \cap f^{-1}[\text{dom} g] = \{x : x \geq 1 \text{ or } x \leq -1\}$ and $g \circ f = \{(x, z) : x \geq 1 \text{ or } x \leq -1 \text{ and, for some } y, x^2 - 1 = y \text{ and } \sqrt{y} = z\} = \langle \sqrt{x^2 - 1} : x \geq 1 \text{ or } x \leq -1\rangle$.
- If f is a function, its inverse f^{-1} is a relation, but it may not be a function.
- We say that a function f is **invertible** if f^{-1} is a function.

Invertibility and Injectivity

Definition (Injective Function)

A function f is called **one-to-one** or **injective** if $a_1 \in \mathrm{dom} f$, $a_2 \in \mathrm{dom} f$, and $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$. I.e., if $a_1 \in \mathrm{dom} f$, $a_2 \in \mathrm{dom} f$, and $f(a_1) = f(a_2)$, then $a_1 = a_2$. Thus, a one-to-one function assigns different values to different elements from its domain.

Theorem

A function is invertible if and only if it is one-to-one. If f is invertible, then f^{-1} is also invertible and $(f^{-1})^{-1} = f$.

- If f is invertible, then f^{-1} is a function. It follows that $f^{-1}(f(a)) = a$ for all $a \in \mathrm{dom} f$. If $a_1, a_2 \in \mathrm{dom} f$ and $f(a_1) = f(a_2)$, we get $f^{-1}(f(a_1)) = f^{-1}(f(a_2))$ and $a_1 = a_2$. So f is one-to-one.
- Let f be one-to-one. If $a \; f^{-1} \; b_1$ and $a \; f^{-1} \; b_2$, we have $b_1 \; f \; a$ and $b_2 \; f \; a$. Therefore, $b_1 = b_2$, and f^{-1} is a function.
- Since $(f^{-1})^{-1} = f$, f^{-1} is also invertible and f^{-1} is also one-to-one.

Examples

- Example: Let $f = \langle \frac{1}{x^2} : x \neq 0 \rangle$. Find f^{-1}.
  As $f = \{(x, \frac{1}{x^2}) : x \neq 0\}$, we get $f^{-1} = \{(\frac{1}{x^2}, x) : x \neq 0\}$. f^{-1} is not a function since $(1, -1) \in f^{-1}$, $(1, 1) \in f^{-1}$. Therefore, f is not one-to-one: $(1, 1) \in f$ and $(-1, 1) \in f$.
- Example: Let $g = \langle 2x - 1 : x \text{ real} \rangle$. Find g^{-1}.
  g is one-to-one: If $2x_1 - 1 = 2x_2 - 1$, then $2x_1 = 2x_2$ and $x_1 = x_2$.
  Since $g = \{(x, y) : y = 2x - 1, x \text{ real}\}$,
  $g^{-1} = \{(y, x) : y = 2x - 1, x \text{ real}\}$. As customary when describing functions, we express the second coordinate (value) in terms of the first:

$$g^{-1} = \{(y, x) : x = \frac{y + 1}{2}, y \text{ real}\}.$$

  Finally, it is usual to denote the first ("independent") variable x and the second ("dependent") variable y. So we change notation:
  $g^{-1} = \{(x, y) : y = \frac{x+1}{2}, x \text{ real}\} = \langle \frac{x+1}{2} : x \text{ real} \rangle$.

Compatible Functions

Definition (Compatibility)

(a) Functions f and g are called **compatible** if $f(x) = g(x)$, for all $x \in \mathrm{dom} f \cap \mathrm{dom} g$.

(b) A set of functions F is called a **compatible system of functions** if any two functions f and g from F are compatible.

Lemma

(a) Functions f and g are compatible if and only if $f \cup g$ is a function.

(b) Functions f and g are compatible if and only if

$$f \restriction (\mathrm{dom} f \cap \mathrm{dom} g) = g \restriction (\mathrm{dom} f \cap \mathrm{dom} g).$$

- Suppose $f \cup g$ is a function. Let $x \in \mathrm{dom} f \cap \mathrm{dom} g$. Then $x(f \cup g)f(x)$ and $x(f \cup g)g(x)$, whence $f(x) = g(x)$.
- Suppose f, g are compatible. Let $x(f \cup g)y_1$ and $x(f \cup g)y_2$.
  - If $x \in \mathrm{dom} \cap \mathrm{dom} g$, then $y_1 = f(x) = g(x) = y_2$.
  - If $x \in \mathrm{dom} f - \mathrm{dom} g$, then $x \ f \ y_1$ and $x \ f \ y_2$, whence $y_1 = y_2$.
  - If $x \in \mathrm{dom} g - \mathrm{dom} f$ a similar argument applies.

Pasting Together Compatible Functions

Theorem

If F is a compatible system of functions, then $\bigcup F$ is a function with $\operatorname{dom}(\bigcup F) = \bigcup\{\operatorname{dom} f : f \in F\}$. The function $\bigcup F$ extends all $f \in F$.

- Functions from a compatible system can be pieced together to form a single function which extends them all.
- Clearly, $\bigcup F$ is a relation. We show it is a function. If $(a, b_1) \in \bigcup F$ and $(a, b_2) \in \bigcup F$, there are functions $f_1, f_2 \in F$ such that $(a, b_1) \in f_1$ and $(a, b_2) \in f_2$. But f_1 and f_2 are compatible, and $a \in \operatorname{dom} f_1 \cap \operatorname{dom} f_2$. So $b_1 = f(a_1) = f(a_2) = b_2$.
- It is clear that $x \in \operatorname{dom}(\bigcup F)$ if and only if $x \in \operatorname{dom} f$, for some $f \in F$.

Product of Indexed Family of Sets

Definition

Let A and B be sets. The set of all functions on A into B is denoted B^A. (Of course, it must first be shown that B^A exists.)

- Let $S = \langle S_i : i \in I \rangle$ be a function with domain I. The values S_i are arbitrary sets. We call the function $\langle S_i : i \in I \rangle$ an **indexed system of sets**, stressing that the values of S are sets.
- Now let $S = \langle S_i : i \in I \rangle$ be an indexed system of sets. We define the **product of the indexed system** S as the set

$$\prod S = \{f : f \text{ is a function on } I \text{ and } f_i \in S_i, \text{ for all } i \in I\}.$$

- Other notations are $\prod \langle S(i) : i \in I \rangle, \prod_{i \in I} S(i), \prod_{i \in I} S_i$.
- If S is such that $S_i = B$, for all $i \in I$, then $\prod_{i \in I} S_i = B^I$.
- The "exponentiation" of sets is related to "multiplication" of sets in the same way as similar operations on numbers are related.

Notation

- Two remarks concerning notation:
  - $\bigcup A$ and $\bigcap A$ were defined for any system of sets A ($A \neq \emptyset$ in case of intersection). Often the system A is given as a range of some function, i.e., of some indexed system. We say that A is **indexed by** S if
$$A = \{S_i : i \in I\} = \text{ran} S,$$
where S is a function on I. It is then customary to write
$$\bigcup A = \bigcup \{S_i : i \in I\} = \bigcup_{i \in I} S_i,$$
and similarly for intersections.
  - Let f be a function on a subset of the product $A \times B$. It is customary to denote the value of f at $(x, y) \in A \times B$ by $f(x, y)$, rather than $f((x, y))$. In this context, we regard f as a function of two variables x and y.

Subsection 4

Equivalences and Partitions

Equivalence Relation on a Set

Definition (Equivalence Relation)

Let R be a binary relation in A.

(a) R is called **reflexive in** A if, for all $a \in A$, $a \; R \; a$.

(b) R is called **symmetric in** A if, for all $a, b \in A$,

$$a \; R \; b \text{ implies } b \; R \; a.$$

(c) R is called **transitive in** A if, for all $a, b, c \in A$,

$$a \; R \; b \text{ and } b \; R \; c \text{ imply } a \; R \; c.$$

(d) R is called an **equivalence on** A if it is reflexive, symmetric, and transitive in A.

Examples

(a) Let P be the set of all people living on Earth. We say that a person p is equivalent to a person q ($p \equiv q$) if p and q live in same country.

- Trivially, $\equiv$ is reflexive, symmetric, and transitive in P.

Notice that the set P can be broken into classes of mutually equivalent elements. All people living in the United States form one class, all people living in France are another class, etc.

- All members of the same class are mutually equivalent;
- Members of different classes are never equivalent.

The equivalence classes correspond exactly to different countries.

(b) Define an equivalence E on the set $\mathbb{Z}$ of all integers as follows:

$$x \; E \; y \text{ if and only if } x - y \text{ is divisible by } 2.$$

I.e., two numbers are equivalent if their difference is even.

- E is reflexive, symmetric and transitive.

Again, the set $\mathbb{Z}$ can be divided into equivalence classes under (or, **modulo**) the equivalence E. In this case, there are two equivalence classes: the set of even integers and the set of odd integers.

- Any two even integers are equivalent; so are any two odd integers.
- But an even integer cannot be equivalent to an odd one.

Equivalence Classes

- Any equivalence on A partitions A into equivalence classes; conversely, given a suitable partition of A, there is an equivalence on A determined by it.

Definition (Equivalence Class)

Let E be an equivalence on A and let $a \in A$. The **equivalence class of** a **modulo** E is the set

$$[a]_E = \{x \in A : x \; E \; a\}.$$

Lemma

Let $a, b \in A$.

(a) a is equivalent to b modulo E if and only if $[a]_E = [b]_E$.

(b) a is not equivalent to b modulo E if and only if $[a]_E \cap [b]_E = \emptyset$.

Proof of the Lemma

(a) $a\ E\ b$ implies $[a]_E = [b]_E$: Assume that $a\ E\ b$. Let $x \in [a]_E$, i.e., $x\ E\ a$. By transitivity, $x\ E\ a$ and $a\ E\ b$ imply $x\ E\ b$, i.e., $x \in [b]_E$. Similarly, $x \in [b]_E$ implies $x \in [a]_E$. So $[a]_E = [b]_E$.
$[a]_E = [b]_E$ implies $a\ E\ b$: Assume that $[a]_E = [b]_E$. Since E is reflexive, $a\ E\ a$, so $a \in [a]_E$. But then $a \in [b]_E$, that is, $a\ E\ b$.

(b) $a \not{E}\ b$ implies $[a]_E \cap [b]_E = \emptyset$: Assume $a\ E\ b$ is not true; we have to prove $[a]_E \cap [b]_E \neq \emptyset$. If not, there is $x \in [a]_E \cap [b]_E$; so $x\ E\ a$ and $x\ E\ b$. But then, using first symmetry and then transitivity, $a\ E\ x$ and $x\ E\ b$, so $a\ E\ b$, a contradiction.
$[a]_E \cap [b]_E = \emptyset$ implies $a \not{E}\ b$: Assume finally that $[a]_E \cap [b]_E = \emptyset$. If a and b were equivalent modulo E, $a\ E\ b$ would hold, so $a \in [b]_E$. But also $a \in [a]_E$, implying $[a]_E \cap [b]_E \neq \emptyset$, a contradiction.

Partition of a Set

Definition (Partition)

A system S of nonempty sets is called a **partition of** A if

(a) S is a system of mutually disjoint sets, i.e., if $C \in S, D \in S$, and $C \neq D$, then $C \cap D = \emptyset$;

(b) The union of S is the whole set A, i.e., $\bigcup S = A$.

Definition (System of Equivalence Classes of an Equivalence Relation)

Let E be an equivalence on A. The system of all equivalence classes modulo E is denoted by A/E: $A/E = \{[a]_E : a \in A\}$.

Theorem (Equivalence Classes Form a Partition)

Let E be an equivalence on A. Then A/E is a partition of A.

- Property (a) follows from the preceding lemma: If $[a]_E \neq [b]_E$, then a and b are not E-equivalent, so $[a]_E \cap [b]_E = \emptyset$.
  To prove (b), notice that $\bigcup A/E = A$ because $a \in [a]_E$. Notice also that no equivalence class is empty, since at least $a \in [a]_E$.

Equivalence of a Partition

- For each partition there is a corresponding equivalence relation.

Definition (Equivalence of a Partition)

Let S be a partition of A. The relation E_S in A is defined by

$$E_S = \{(a,b) \in A \times A : \text{there is } C \in S, \text{ such that } a \in C \text{ and } b \in C\}.$$

Objects a and b are related by E_S if and only if they belong to the same set from the partition S.

Theorem

Let S be a partition of A. Then E_S is an equivalence on A.

(a) Reflexivity: Let $a \in A$. Since $A \in \bigcup S$, there is $C \in S$ for which $a \in C$, so $(a,a) \in E_S$.

(b) Symmetry: Assume $a \; E_S \; b$. Then there is $C \in S$, for which $a \in C$ and $b \in C$. Then, of course, $b \in C$ and $a \in C$, so $b \; E_S \; a$.

(c) Transitivity: Assume $a \; E_S \; b$ and $b \; E_S \; c$. Then there are $C \in S$ and $D \in S$, such that $a \in C$ and $b \in C$ and $b \in D$ and $c \in D$. We see that $b \in C \cap D$, so $C \cap D \neq \emptyset$, i.e., $C = D$. So $a \in C$, $c \in C$, and $a \; E_S \; c$.

Equivalence Relations and Partitions

Theorem (Equivalence Relations and Partitions)

(a) If E is an equivalence on A and $S = A/E$, then $E_S = E$.

(b) If S is a partition of A and E_S is the corresponding equivalence, then $A/E_S = S$.

- Equivalences and partitions describe the same "mathematical reality":
  - Every equivalence E determines a partition $S = A/E$. The equivalence E_S determined by this partition S is identical with the original E.
  - Conversely, each partition S determines an equivalence E_S; when we form equivalence classes modulo E_S, we recover the original partition S.

Definition (Set of Representatives)

A set $X \subseteq A$ is called a **set of representatives for the equivalence** E_S (or **for the partition** S of A) if, for every $C \in S$, $X \cap C = \{a\}$, for some $a \in C$.

- The Axiom of Choice is required to ensure that every partition has some set of representatives.

Subsection 5

Orderings

Partial Orderings

Definition (Antisymmetry)

A binary relation R in A is **antisymmetric** if, for all $a, b \in A$,

$$a \; R \; b \text{ and } b \; R \; a \text{ imply } a = b.$$

Definition (Partial Ordering)

A binary relation R in A which is reflexive, antisymmetric and transitive is called a **(partial) ordering** of A. The pair (A, R) is called an **ordered set**.

- $a \; R \; b$ can be read as "a is less than or equal to b" or "b is greater than or equal to a" (in the ordering R).
- By reflexivity, every element of A is less than or equal to itself.
- By antisymmetry, if a is less than or equal to b, and, at the same time, b is less than or equal to a, then $a = b$.
- Finally, by transitivity, if a is less than or equal to b and b is less than or equal to c, a has to be less than or equal to c.

Examples of Orderings

(a) $\leq$ is an ordering on the set of all (natural, rational, real) numbers.

(b) Define the relation $\subseteq_A$ in A as follows:

$$x \subseteq_A y \quad \text{if and only if} \quad x \subseteq y \text{ and } x, y \in A.$$

Then $\subseteq_A$ is an ordering of the set A.

(c) Define the relation $\supseteq_A$ in A as follows:

$$x \supseteq_A y \quad \text{if and only if} \quad x \supseteq y \text{ and } x, y \in A.$$

Then $\supseteq_A$ is also an ordering of the set A.

(d) The relation $\mid$ defined by:

$$n \mid m \quad \text{if and only if} \quad n \text{ divides } m$$

is an ordering of the set of all positive integers.

(e) The relation Id_A is an ordering of A.

Strict Orderings

Definition (Asymmetry)

A relation S in A is **asymmetric** if $a\ S\ b$ implies that $b\ S\ a$ does not hold, for any $a, b \in A$. That is, $a\ S\ b$ and $b\ S\ a$ can never both be true.

Definition (Strict Ordering)

A relation S in A is a **strict ordering** if it is asymmetric and transitive.

Theorem

(a) Let R be an ordering of A. Then the relation S defined in A by
$$a\ S\ b \quad \text{if and only if} \quad a\ R\ b \text{ and } a \neq b$$
is a strict ordering of A.

(b) Let S be a strict ordering of A. Then the relation R defined in A by
$$a\ R\ b \quad \text{if and only if} \quad a\ S\ b \text{ or } a = b$$
is an ordering of A.

We say that the strict ordering S **corresponds** to the ordering R and vice versa.

Proof of the Theorem

(a) Let us show that S is asymmetric: Assume that both $a\ S\ b$ and $b\ S\ a$ hold for some $a, b \in A$. Then also $a\ R\ b$ and $b\ R\ a$, so $a = b$ (because R is antisymmetric). This contradicts the definition of $a\ S\ b$.
Next, we show that S is transitive: If $a\ S\ b$ and $b\ S\ c$, then $a\ R\ b$ and $a \neq b$ and $b\ R\ c$ and $b \neq c$.
- By the transitivity of R, $a\ R\ c$;
- $a \neq c$, since, if $a\ R\ b$ and $b\ R\ a$, then $a = b$ a contradiction.

Therefore, $a\ S\ c$ and S is transitive.

(b) Let us show that R is reflexive: Since $a = a$, for all a, $a\ R\ a$.
Let us show that R is antisymmetric: Assume that $a\ R\ b$ and $b\ R\ a$. Since S is asymmetric, we conclude that $a = b$.
For transitivity, assume $a\ R\ b$ and $b\ R\ c$. Then $a\ S\ b$ or $a = b$ and $b\ S\ c$ or $b = c$.
- If $a\ S\ b$ and $b\ S\ c$, then $a\ S\ c$ by the transitivity of S.
- If $a\ S\ b$ and $b = c$, then $a\ S\ c$.
- If $a = b$ and $b\ S\ c$, then $a\ S\ c$.
- If $a = b$ and $b = c$, then $a = c$.

Comparable and Incomparable Elements

Definition (Comparable and Incomparable Elements)

Let $a, b \in A$, and let $\leq$ be an ordering of A. We say that a and b are **comparable** in the ordering $\leq$ if $a \leq b$ or $b \leq a$.
We say that a and b are **incomparable** if they are not comparable, i.e., if neither $a \leq b$ nor $b \leq a$ holds.
Both definitions can be stated equivalently in terms of the corresponding strict ordering $<$. For example, a and b are incomparable in $<$ if $a \neq b$ and neither $a < b$ nor $b < a$ holds.

- Example:
  (a) Any two real numbers are comparable in the ordering $\leq$.
  (b) 2 and 3 are incomparable in the ordering $|$.
  (c) Any two distinct $a, b \in A$ are incomparable in Id_A.
  (d) If the set A has at least two elements, then there are incomparable elements in the ordered set $(\mathcal{P}(A), \subseteq_{\mathcal{P}(A)})$.

Linear or Total Orderings

Definition (Linear or Total Ordering)

An ordering $\leq$ (or $<$) of A is called **linear** or **total** if any two elements of A are comparable. The pair $(A, \leq)$ is then called a **linearly ordered set**.

- Example: The ordering $\leq$ of positive integers is total, while $|$ is not.

Definition (Chain)

Let $B \subseteq A$, where A is ordered by $\leq$. B is a **chain** in A if any two elements of B are comparable.

- Example: The set of all powers of 2 (i.e., $\{2^0, 2^1, 2^2, 2^3, \ldots\}$) is a chain in the set of all positive integers ordered by $|$.

Least, Minimal, Greatest and Maximal Elements

Definition (Least, Minimal, Greatest, Maximal)

Let $\leq$ be an ordering of A, and let $B \subseteq A$.

(a) $b \in B$ is the **least element of** B in the ordering $\leq$ if $b \leq x$, for every $x \in B$.

(b) $b \in B$ is a **minimal element of** B in the ordering $\leq$ if there exists no $x \in B$ such that $x \leq b$ and $x \neq b$.

(a') Similarly, $b \in B$ is the **greatest element of** B in the ordering $\leq$ if, for every $x \in B$, $x \leq b$.

(b') $b \in B$ is a **maximal element of** B in the ordering $\leq$ if there exists no $x \in B$ such that $b \leq x$ and $x \neq b$.

Some Examples

- Example: Let $\mathbb{N}$ be the set of positive integers ordered by the divisibility relation $|$.
  - 1 is the least element of $\mathbb{N}$;
  - $\mathbb{N}$ has no greatest element.
- Example: Let B be the set of all positive integers greater (in magnitude) than 1, $B = \{2, 3, 4, \ldots\}$.
  - B does not have a least element in $|$ (e.g., 2 is not the least element because $2 \mid 3$ fails).
  - It has, however, (infinitely) many minimal elements: numbers 2, 3, 5, etc. (exactly all prime numbers) are minimal.
  - B has neither greatest nor maximal elements.

Properties of Least and Minimal Elements

Theorem

Let A be ordered by $\leq$, and let $B \subseteq A$.

(a) B has at most one least element.

(b) The least element of B (if it exists) is also minimal.

(c) If B is a chain, then every minimal element of B is also least.

The theorem remains true if the words "least" and "minimal" are replaced by "greatest" and "maximal", respectively.

(a) If both b_1 and b_2 are least elements of B, then $b_1 \leq b_2$ and $b_2 \leq b_1$. Thus, by antisymmetry, $b_1 = b_2$.

(b) If b is not minimal, then there exists $x \in B$, such that $x < b$. Therefore, $b \not\leq x$ and b is not the least element in B.

(c) Suppose b is minimal in B. Let $x \in B$. Since B is a chain, $b \leq x$ or $x \leq b$. If $x \leq b$, since b is minimal, we must have $x = b$. Thus, in either case, $b \leq x$ and b is the least element in B.

Lower and Upper Bounds, Infima and Suprema

Definition (Lower, Upper Bounds, Infimum, Supremum)

Let $\leq$ be an ordering of A, and let $B \subseteq A$.

(a) $a \in A$ is a **lower bound of** B in the ordered set $(A, \leq)$ if $a \leq x$, for all $x \in B$.

(b) $a \in A$ is called an **infimum of** B in $(A, \leq)$ (or the **greatest lower bound of** B in $(A, \leq)$) if it is the greatest element of the set of all lower bounds of B in $(A, \leq)$.

Similarly,

(a') $a \in A$ is an **upper bound of** B in the ordered set $(A, \leq)$ if $x \leq a$, for all $x \in B$.

(b') $a \in A$ is called a **supremum of** B in $(A, \leq)$ (or the **least upper bound of** B in $(A, \leq)$) if it is the least element of the set of all upper bounds of B in $(A, \leq)$.

- Note that the difference between the least element of B and a lower bound of B is that the second notion does not require $b \in B$.

Properties of Infima and Suprema

Theorem

Let $(A, \leq)$ be an ordered set and let $B \subseteq A$.

(a) B has at most one infimum.

(b) If b is the least element of B, then b is the infimum of B.

(c) If b is the infimum of B and $b \in B$, then b is the least element of B.

(d) $b \in A$ is an infimum of B in $(A, \leq)$ if and only if

  (i) $b \leq x$, for all $x \in B$.

  (ii) If $b' \leq x$, for all $x \in B$, then $b' \leq b$.

The theorem remains true if the words "least" and "infimum" are replaced by the words "greatest" and "supremum" and "$\leq$" is replaced by "$\geq$" in (i) and (ii).

(b) The least element b of B is certainly a lower bound of B. If b' is any lower bound of B, $b' \leq b$ because $b \in B$. So b is the greatest element of the set of all lower bounds of B.

Notation and Examples

- We use notations $\inf(B)$ and $\sup(B)$ for the infimum of B and the supremum of B, if they exist.
- If B is linearly ordered, we also use $\min(B)$ and $\max(B)$ to denote the minimal (least) and the maximal (greatest) elements of B, if they exist.
- Example: Let $\leq$ be the usual ordering of the set of real numbers. Let $B_1 = \{x : 0 < x < 1\}$, $B_2 = \{x : 0 \leq x < 1\}$, $B_3 = \{x : x > 0\}$, and $B_4 = \{x : x < 0\}$.
  - Then B_1 has no least element and no greatest element. Any $b \leq 0$ is a lower bound of B_1, so 0 is the greatest lower bound of B_1, i.e., $0 = \inf(B)$. Similarly, any $b \geq 1$ is an upper bound of B_1, so $1 = \sup(B_1)$.
  - The set B_2 has a least element. So $0 = \min(B_2) = \inf(B_2)$. It does not have a greatest element. Nevertheless, $\sup(B_2) = 1$.
  - The set B_3 has neither a greatest element nor a supremum (actually B_3 has no upper bound in $\leq$). Of course, $\inf(B_3) = 0$.
  - Similarly, B_4 has no lower bounds, hence no infimum.

Order Isomorphisms

Definition (Order Isomorphism)

An **isomorphism** between two ordered sets $(P, <)$ and $(Q, \prec)$ is a one-to-one function h with domain P and range Q such that, for all $p_1, p_2 \in P$, $\quad p_1 < p_2 \quad$ if and only if $\quad h(p_1) \prec h(p_2)$.
If an isomorphism exists between $(P, <)$ and $(Q, \prec)$, then $(P, <)$ and $(Q, \prec)$ are **isomorphic**.

Lemma

Let $(P, <)$ and $(Q, \prec)$ be linearly ordered sets, and let h be a one-to-one function with domain P and range Q such that $h(p_1) \prec h(p_2)$ whenever $p_1 < p_2$. Then h is an isomorphism between $(P, <)$ and $(Q, \prec)$.

- We have to verify that if $p_1, p_2 \in P$ are such that $h(p_1) \prec h(p_2)$, then $p_1 < p_2$. But if p_1 is not less than p_2, then, because $<$ is a linear ordering of P, either $p_1 = p_2$ or $p_2 < p_1$. If $p_1 = p_2$, then $h(p_1) = h(p_2)$ and, if $p_2 < p_1$, then $h(p_2) \prec h(p_1)$, by the assumption. Either case contradicts $h(p_1) \prec h(p_2)$.