UMA205: Introduction to Algebraic Structures

Naman Mishra

January 2024

Contents

1 **Lecture 03:** Mon 08 Jan '24

1 Axioms of Set Theory (ZFC)

Definition 1.1 (Set)**.** A set is a well-defined collection of objects, which we call elements. We will write $x \in A$ to say that x is an element of A.

Well-defined means that given any object, we can state without ambiguity whether it is an element of the set or not.

Axiom 1.1. Sets are themselves objects. If A and B are sets, it is meaningful to ask whether A is an element of B.

Axiom 1.2 (Extensionality)**.** Two sets A and B are equal, written $A = B$, if every element of A is a member of B and vice versa.

Axiom 1.3 (Existence)**.** There exists a set, denoted by $\varnothing$ or $\{\}$, known as the empty set, which does not contain any elements, *i.e.*, $x \notin \varnothing$ for all objects x.

Problem 0.1. $\varnothing$ is unique.

Proof. Suppose $\varnothing$ and $\varnothing'$ are both empty sets. Then $x \in \varnothing \iff x \in \varnothing'$

since both are always false. □

Lemma 1.2 (Single choice)**.** Let A be a non-empty set. Then there exists an object x such that $x \in A$.

Proof. If not, then $x \notin A$ for all objects x and so $A = \varnothing$. □

Thus, we can choose an element of A to certify its non-emptiness.

Axiom 1.4 (Pairing)**.** If a is an object, there exists a set, denoted $\{a\}$, whose only element is a. Similarly, if a and b are objects, there exists a set, denoted $\{a, b\}$, whose only elements are a and b.

For example, we can now construct $\varnothing$, $\{\varnothing\}$, $\{\{\varnothing\}\}$, $\{\varnothing, \{\varnothing\}\}$, etc, all of which are distinct.

Axiom 1.5 (Pairwise union)**.** Given sets A and B, there exists a set, denoted $A \cup B$, called the union of A and B, which consists of exactly the elements in A, B, or both.

Problem 0.2. $A \cup B = B \cup A$.

Proof. By commutativity of $\vee$. □

Problem 0.3. $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof. By associativity of $\vee$. □

Definition 1.3 (Subset)**.** A is a subset of B if every element of A is alaso an element of B, denoted $A \subseteq B$.

Axiom 1.6 (Specification)**.** (also called Separation). Let A be a set and let $P(x)$ be a property for every $x \in A$. Then there exists a set $S = \{x \in A \mid P(x)\}$ where $x \in S$ iff $x \in A$ and $P(x)$ is true.

We can now define the intersection, $A \cap B$, and difference, $A \setminus B$, of sets A and B.

Definition 1.4. Let A and B be sets. we define the intersection $A \cap B = \{x \in A \mid x \in B\}$ and the difference $A \setminus B = \{x \in A \mid x \notin B\}$.

A and B are said to be disjoint if $A \cap B = \varnothing$.

Recall that sets form a Boolean algebra under the operations $\cup$, $\cap$, and $\setminus$. For example, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, de Morgan's laws, etc.

Axiom 1.7 (Replacement)**.** Let A be a set and let $P(x, y)$ be a property for every $x \in A$ and every object y, such that for every $x \in A$ there is at most one y for which $P(x, y)$ is true. Then there exists a set $S = \{y \mid P(x, y) \text{ is true for some } x \in A\}$. That is, $y \in S$ iff $P(x, y)$ is true for some $x \in A$.

Examples.

- Let $A = \{7, 9, 22\}$ and $P(x, y) \equiv y = x_{++}$. Then $S = \{8, 10, 23\}$.
- Let $A = \{7, 9, 22\}$ and $P(x, y) \equiv y = 1$. Then $S = \{1\}$.

Axiom 1.8 (Infinity)**.** There exists a set, denoted $\mathbb{N}$, whose objects are called natural numbers, *i.e.*, an object $0 \in \mathbb{N}$, and n_{++} for every $n \in \mathbb{N}$, such that the Peano axioms hold.

Axiom 1.9 (Foundation)**.** (also called Regularity). If A is a non-empty set, then there exists at least one $x \in A$ which is either not a set or is disjoint from A.

For example, if $A = \{\{1, 2\}, \{1, 2, \{1, 2\}\}\}$, then $\{1, 2\}$ is an element of A which is disjoint from A.

Lecture 04: Wed 10 Jan '24

Definition 1.5 (Cartesian product)**.** Let A and B be sets. Then $A \times B = \{(a, b) \mid a \in A, b \in B\}$ is called the *Cartesian product* of A and B.

This exists by virtue of the axiom of powers (1.10).

Definition 1.6 (Relation)**.** Let A and B be sets. Then a subset R of $A \times B$ is called a (binary) *relation* from A to B. If $B = A$, we say that R is a relation on A.

We define some properties of relations.

Definition 1.7. Let R be a relation on a set A. We say that R is

(i) **reflexive** if $(a, a) \in R$ for all $a \in A$,

(ii) **symmetric** if $(a, b) \in R \implies (b, a) \in R$,

(iii) **antisymmetric** if $(a, b) \in R \wedge (b, a) \in R \implies a = b$,

(iv) **transitive** if $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$.

If R satisfies (i), (ii) and (iv), it is said to be an *equivalence relation*. We write $a \sim_R b$ for $(a, b) \in R$.

If R satisfies (i), (iii) and (iv), it is a partial order. We write $a \leq_R b$ or $a \geq_R b$ for $(a, b) \in R$.

Definition 1.8 (Equivalence class)**.** Let X be a set and $\sim_R$ an equivalence relation on X. The equivalence class associated with $x \in X$ is

$$[x] = \{y \in X \mid y \sim_R x\}.$$

Definition 1.9 (Partition)**.** A (set) *partition* of a set X is a family $\{X_\alpha \mid \alpha \in I\}$, where I is some indexing set, such that,

(i) $X_\alpha \cap X_\beta = \varnothing$ for all $\alpha \neq \beta \in I$,

(ii) $\bigcup_{\alpha \in I} X_\alpha = X$.

This is also written as simply

$$\bigsqcup_{\alpha \in I} X_\alpha = X.$$

Proposition 1.10 (Fundamental theorem of equivalence relations)**.** Let X be a set and $\sim_R$ an equivalence relation on X. Then the family of equivalence classes $\{[x] \mid x \in X\}$ forms a partition of X. Conversely, every partition arises from an equivalence relation.

Proof. Exercise. □

Definition 1.11. Let X be a set and $\sim_R$ an equivalence relation on X. Then the set $X/\sim_R = \{[x] \mid x \in X\}$ is called the *quotient set* of X by R.

Examples.

- Consider $\mathbb{N}$ with the relation $a \sim_R b \iff a \equiv b \pmod 3$. The quotient set $\mathbb{N}/R$ is $\{[0], [1], [2]\}$, which is morally the same as $\{0, 1, 2\}$.
- For any set A with the equality relation $=$, the quotient set $A/=$ is the (morally) the same as A.
- Consider $\mathbb{R}^2$ with $(x, y) \sim (z, w)$ if $x^2 + y^2 = z^2 + w^2$. Then $\mathbb{R}^2/\sim = \{[(r, 0)] \mid r \in \mathbb{R}\}$ which is morally just the set of non-negative reals.

Definition 1.12 (Function)**.** Let A and B be sets. A relation f from A to B is said to be a *function* if for all $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$.

A is said to be the *domain*, B is said to be the *range* or *codomain* of f. For a subset $C \subseteq A$, the image of C under f is $f(C) = \{f(a) \mid a \in C\}$.

For a subset $D \subseteq B$, the *preimage* or *inverse image* of D under f is $f^{-1}(D) = \{a \in A \mid f(a) \in D\}$.

Note that $f(C)$ exists by the axiom of replacement.

Examples.

- $A = B = \mathbb{N}$, $f(a) = a_{++}$. Then $f(\mathbb{N}) = \mathbb{N} \setminus \{0\}$.

$$f^{-1}(\{a\}) = \begin{cases} \{a - 1\} & \text{if } a > 0 \\ \varnothing & \text{if } a = 0 \end{cases}$$

Definition 1.13. Two functions f and g with the same domain X and range Y are equal if $f(x) = g(x)$ for all $x \in X$.

Definition 1.14 (Composition)**.** If $f : X \to Y$ and $g : Y \to Z$, then the *composition* $g \circ f$ is a function $g \circ f \colon X \to Z$ given by

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

Lecture 05: Fri 12 Jan '24

Definition 1.15. A function $f \colon A \to B$ is said to be

- *injective*, if $f(x) = f(y)$ implies $x = y$,
- *surjective*, if $f(A) = B$,
- *bijective*, if it is both injective and surjective.
- an *involution*, if $f(f(x)) = x$ for all $x \in A$.

Exercise 1.16. Let $f\colon A \to B$ be an involution. Show that f is bijective.

Solution. f is surjective since everything is in the range. Injective since $f(x) = f(y) \implies f(f(x)) = f(f(y)) \implies x = y$.

A function is bijective iff for any $b \in B$ there is a unique $a \in A$ such that $f(a) = b$.

Definition 1.17. Let $f\colon A \to B$ be bijective. The *inverse* of f is the function $f^{-1}\colon B \to A$ where $f^{-1}(b)$ is the unique $a \in A$ such that $f(a) = b$.

Axiom 1.10 (Powers)**.** Let X and Y be sets. Then there exists a set, denoted Y^X, consisting of all functions from $X \to Y$.

Exercise 1.18. Let X be a set. Then $\{Y \mid Y \subseteq X\}$ is also a set.

Solution. The property $P(F, X_F)$ given by

$$P(F, X_F) \iff F \in 2^X \wedge X_F = \{x \in X \mid F(x) = 1\}$$

is satisfied by at most one X_F for any F. Thus applying the axiom of replacement on 2^S gives the desired set.

Axiom 1.11 (Unions)**.** Let A be a set whose elements are also sets. Then there exists a set, denoted $\bigcup A$, whose elements are the elements of the elements of A. Thus $x \in \bigcup A \iff x \in S$ for some $S \in A$.

Remarks. This axiom implies axiom 1.5.

Let I be a set such that A_α is a set for all $\alpha \in I$. Then $\{A_\alpha \mid \alpha \in I\}$ is a set by the axiom of replacement. Thus $\bigcup_{\alpha \in I} A_\alpha$ is a set.

Definition 1.19. Two sets X and Y are said to have the same *cardinality* if there exists a bijection $f\colon X \to Y$.

Let $n \in \mathbb{N}$. If a set X has the same cardinality as $\{0, 1, \ldots, n-1\}$, then X is said to be *finite* and have cardinality n.

Definition 1.20. A set X is *countably infinite* or *countable* if it has the same cardinality as $\mathbb{N}$, is *at most countable* if it is finite or countable, and is *uncountable* otherwise.

Exercise 1.21. Let $m < n$ be naturals. Show that there is

(i) no surjection from $[m]$ to $[n]$[1].

(ii) no injection from $[n]$ to $[m]$.

(iii) a bijection from $[a]$ to $[b]$ iff $a = b$.

Exercise 1.22 (Properties of countable sets)**.**

(i) If X and Y are countable, then so is $X \cup Y$.

(ii) The set $\{(n, m) \in \mathbb{N} \times \mathbb{N} \mid 0 \leq m \leq n\}$ is countable.

(iii) $\mathbb{N} \times \mathbb{N}$ is countable.

Theorem 1.23. Let X be an arbitrary set. Then X and 2^X cannot have the same cardinality.

Proof. Let $f \colon X \to 2^X$. Consider $A = \{x \in X \mid x \notin f(x)\} \subseteq X$. So $A \in 2^X$. Since for any $x \in X$, $x \in A \iff x \notin f(x)$, we have $f(x) \neq A$ for all $x \in X$. Thus f is not surjective. □

[1] $[n] = \{1, \ldots, n\}$