UMA205: Introduction to Algebraic Structures

Naman Mishra

January 2024

Contents

Lecture 04: Wed 10 Jan '24

> **Definition 0.1** (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 (0.1).

> **Definition 0.2** (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 0.3.** 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 $(a, b) \in R \land (b, a) \in R \implies a = b$,
>
> (iv) **transitive** if $(a, b) \in R \land (b, c) \in R \implies (a, c) \in R$.
>
> 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 0.4 (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 0.5 (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 0.6 (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 0.7. 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 0.8 (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 0.9. 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 0.10 (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 0.11. 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 0.12. 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 0.13. 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 0.1 (Powers)**.** Let X and Y be sets. Then there exists a set, denoted Y^X, consisting of all functions from $X \to Y$.

Exercise 0.14. 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 0.2 (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 **??**.

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 0.15. 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 0.16. 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 0.17. 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 0.18 (Properties of countable sets)**.**

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

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

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

Theorem 0.19. 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. $\square$

Lecture 06: Mon 15 Jan '24

News: Quiz 1 tomorrow. Material upto and including lecture 6.

Definition 0.20. Let I be a possibly infinite indexing set and for all $\alpha \in I$ let X_α be a set. Then its (possibly infinite) Cartesian product is defined as

$$\prod_{\alpha \in I} X_\alpha = \left\{ (x_\alpha)_{\alpha \in I} \in \Big(\bigcup_{\beta \in I} X_\beta \Big)^I \;\middle|\; x_\alpha \in X_\alpha \text{ for all } \alpha \in I \right\}$$

Exercise 0.21. For any sets I and X, $\prod_{\alpha \in I} X = X^I$.

Axiom 0.3 (Choice)**.** Let I be a set and for all $\alpha \in I$ let $X_\alpha \neq \varnothing$. Then $\prod_{\alpha \in I} X_\alpha$ is non-empty.

Definition 0.22. A *choice function* on X is a function $f\colon 2^X \setminus \varnothing \to X$ such that for all non-empty $S \subseteq X$, $f(S) \in S$.

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

Fact 0.23. The existence of a choice function for every X is equivalent to the axiom of choice.

Remarks. A variant of AoC is the *axiom of countable choice*, which requires I to be at most countable.

Lemma 0.24. Let E be a bounded above non-empty subset of $\mathbb{R}$. Then there exists a sequence $(a_n)_{n\in\mathbb{N}}$ such that $a_n \in E$ for all n and $\lim_{n\to\infty} a_n = \sup E$.

Proof. Let $X_n = \left\{x \in E \mid \sup E - \frac{1}{n} \leq x \leq \sup E\right\}$. Each X_n is non-empty. By AoC, there exists a sequence $(a_n)_{n\in\mathbb{N}}$ such that for all n, $a_n \in X_n$. Thus $a_n \in E$ for all n and $\lim_{n\to\infty} a_n = \sup E$. □

Definition 0.25. Let $(P, \leq)$ be a poset. A subset $Y \subseteq P$ is called a *chain* or *totally ordered* if for any $y, y' \in Y$, either $y \leq y'$ or $y' \leq y$.

Definition 0.26. Let $(P, \leq)$ be a poset and $Y \subseteq P$. We say that y is a *minimal* (resp. *maximal*) element of Y if there is no $y' \in Y$ such that $y' < y$ (resp. $y' > y$).

Definition 0.27. Let $(P, \leq)$ be a poset and $Y \subseteq P$ be a chain. We say that Y is *well-ordered* if every non-empty subset of Y has a minimal element.

Axiom 0.3 (Well-ordering principle)**.** Given any set X, there exists a well-ordering on X.

Axiom 0.3 (Zorn's lemma)**.** Let $(X, \leq)$ be a non-empty poset such that every chain Y of X has an upper bound (there exists an $x \in X$ such that $y \leq x$ for all $y \in Y$). Then X has a maximal element.

Fact 0.28. The axiom of choice, well-ordering principle, and Zorn's lemma are equivalent.

Proof. **Zorn $\implies$ AoC.** Let $X \neq \varnothing$ and let P be the set of ordered pairs (Y, f) where $Y \subseteq X$ and f is a choice function on Y. Define

$(Y, f) \leq (Y', f')$ if $Y \subseteq Y'$ and $f'|_Y = f$. P is non-empty because $\{x\} \subseteq X$ has a choice function for all $x \in X$.

Let C be a chain in P. Then let $\overline{Y} = \bigcup_{(Y,f) \in C} Y$ and define $\overline{f}$ by setting $\overline{f}(S) = f(S)$ for any f for which $f(S)$ is defined. Then $(\overline{Y}, \overline{f})$ is an upper bound for C.

By Zorn's lemma, there exists a maximal element of P, say (Y, f). If $x \in X \setminus Y$, we can extend f to $Y \cup \{x\}$ by defining $f(S) = x$ for any S containing x. This contradicts the maximality of (Y, f). Thus $X \setminus Y$ must be empty, and so f is a choice function on X.

AoC $\implies$ Zorn. Let P be a poset whose every chain has an upper bound. Suppose P has no maximal element. Pick $x_0 \in P$ using a choice function. Since x_0 is not maximal, there exists an x_1 larger than x_0, and x_2 larger than x_1, and so on. This gives a chain $x_0 < x_1 < x_2 < \ldots$. But then x_ω is an upper bound for this chain. This gives another chain $x_\omega < x_{\omega+1} < \ldots$. But then $x_{2\omega}$ is an upper bound for this chain.

Continuing in this way, we get a chain which is "larger" than P itself, a contradiction.

$\square$