Math 135 Lecture Notes
Theory of Sets

Professor: Thomas Scanlon
Scribe: Liam Tan

Spring 2024

Contents

1 Introduction to the Theory of Sets

We will formalize set theory and prove theorems based on the constructions from the axioms. The theory we will be developing is called ZFC (Zermelo-Fraenkel Set Theory with Choice). ZFC is a first-order logical theory expressed in the language of set theory called

$$\mathscr{L}(\epsilon)$$

ϵ is the only non-logical symbol, called a binary relation, "$a \in b$".

Where a and b are variables, we can combine atomic formula, logical formula, and quantifiers to form our language. Atomic formula include $a = b$ and $a \in b$. Logical formula include $a \implies b$, $\neg a$, $a \wedge b$, $a \vee b$, $a \iff b$. Quantifiers are $\exists x\varphi$ and $\forall x\varphi$.

An $\mathscr{L}(\epsilon)$-structure is a nonempty set V together with a set $\epsilon \subset V \times V$. For $a, b \in V$

$$(V, \epsilon^V) \models a \in b \iff (a, b) \in \epsilon^V$$

Example 1.1 (The universe of sets).

$$(\mathbb{V}, \epsilon)$$

Theorem 1.1 (ZFC cannot prove that there is a model of ZFC). *i.e. a set V and a set $\epsilon^V \subseteq V \times V$ s.t every axiom of ZFC is true.*

Theorem 1.2 (Godel's Incompleteness Theorem for ZFC). *If ZFC can prove that ZFC is consistent then ZFC is inconsistent*

1.1 Introducing the Axioms

Axiom 1.1 (Axiom of Extensionality). *This axiom defines what it means for two sets to be the same. The equality operator is taken to be primitive in first-order logic and we need to define how it relates to the other symbols.*

$$\forall A \forall B[A = B \iff \forall t[t \in A \iff t \in B]]$$

Example 1.2 (An example of a structure).

$$V = \{0, 1\}$$

$$\epsilon^V = \{(0, 0), (0, 1)\}$$

$$V \models 0 \in 1$$

$$V \models 0 \in 0$$

$(V, \epsilon^V) \not\models$ the axiom of extensionality.

$$V \models \neg(0 = 1)$$

but

$$V \models \forall t[t \in 0 \iff t \in 1]$$

Axiom 1.2 (Empty Set Axiom)**.** *There exists an empty set.*

$$\exists x \forall t \neg[t \in x]$$

We can abbreviate this with the following

$$\exists x \forall t(t \notin x)$$

Definition 1.1 (Defining the $\notin$ symbol)**.** We want to define formula that aren't strictly part of our language. Let us define the negation of the set membership.

$$\Delta_{\notin} : \forall x \forall y[x \notin y \iff \neg(x \in y)] \in \mathscr{L}(\epsilon, \not\epsilon)$$

Proposition 1.1. *For any $\mathscr{L}(\epsilon)$ structure (M, ϵ^M), there is unique expansion $(M, \epsilon^M, /\epsilon^M) \models \Delta_{\notin}$*

Remark 1.1 (Introducing Symbols)**.** We will want to introduce many new symbols throughout the course of this class. e.g. $\subseteq, \mathcal{P}\mathbb{A}$. We will need to define new symbols logically each time we introduce them and can do so hierarchically with previously defined symbols.

Example 1.3 (A structure consistent with the Axioms)**.**

$$V = \{0\}$$

$$\epsilon^V = \emptyset$$

$(V, \epsilon^V) \models$ Empty Set and Extensionality Axioms

Proposition 1.2 (Uniqueness of the Empty Set)**.** *There is exactly one empty set.*

Proof. By the Empty Set Axiom, there is at least one empty set. If x and y are two empty sets. i.e. $(\forall t)t \notin x$ and $(\forall t)t \notin y$, then $\forall t(t \in x \iff t \in y)$. By the Axiom of Extensionality, $x = y$ $\square$

Definition 1.2 (Empty Set Formula)**.**

$$\Delta_{\emptyset} : \forall x[x = \emptyset \iff \forall t(t \notin x)] \in \mathscr{L}(\epsilon, \not\epsilon, \emptyset)$$

where the ϵ and $\not\epsilon$ are binary relation symbols and the $\emptyset$ symbol is called a constant symbol.

Definition 1.3 (Subset Formula).

$$\Delta_{\subseteq} : \forall x \forall y [x \subseteq y \iff \forall t [t \in x \implies t \in y]]$$

Axiom 1.3 (Power Set Axiom).

$$\forall x \exists z \forall t [t \in z \iff t \subseteq x]$$

Proposition 1.3 (Uniqueness of the Power Set). *$\forall x$ there is a unique power set of x*

Definition 1.4 (Power Set Operation).

$$\Delta_{\mathcal{P}} : \forall x \forall z [z = \mathcal{P}x \iff \forall t [t \in z \iff t \subseteq x]]$$

$\mathcal{P}$ is a unary function symbol.

Example 1.4 (What Sets can we build so far). $\emptyset, \mathcal{P}(\emptyset) = \{\emptyset\}, \mathcal{P}\mathcal{P}\emptyset = \{\emptyset, \{\emptyset\}\}$, etc We can keep iterating powersets. We will need to add more axioms. For example, we cannot prove the existence of $\{\{\emptyset\}\}$ with the axioms we have so far.

Axiom 1.4 (Pair Set Axiom).

$$\forall x \forall y \exists z \forall t [t \in z \iff (t = x \vee t = y)]$$

Definition 1.5 (Pair Set Operation).

$$\Delta_{\{,\}} : \forall x \forall t \forall z [z = \{x, y\} \iff \forall t [t \in z \iff t = z \vee t = y]]$$

Example 1.5 (Singleton Set).

$$x = y$$

$$\{x, y\} = \{x, x\} = \{x\}$$

Proposition 1.4 (Existence of the Singleton).

$$\forall x \exists z \forall t [t \in z \iff t = x]$$

Proof. We can apply the Pair Set Axiom with $y = x$ □

Definition 1.6 (Singleton Operation).

$$\Delta_{\{\}} = \forall x \forall y [z = \{x\} \iff \forall t [t \in z \iff t = x]]$$

Example 1.6 (Triplet Set). Can we create a set with three items? We can attempt to apply the pair set axiom to $\{a\}$ and $\{b, c\}$, but unfortunately we will end up with $\{\{a\}, \{b, c\}\}$. We will need to define the union.

Axiom 1.5 (Binary Union Axiom (Not ZFC))**.**

$$\forall x \forall y \exists z \forall t [t \in z \iff (t \in x \vee t \in y)]$$

Definition 1.7 (Binary Union Operation)**.**

$$\Delta_{\cup} : \forall x \forall y \forall z [z = x \cup y \iff \forall t [t \in z \iff (t \in x \vee t \in y)]]$$

Example 1.7 (Triplet Set Reprise)**.** Now with the binary union axiom, we can apply the operation to $\{a\}$ and $\{b, c\}$, which were found by the pair set axiom. Using the Binary Union Axiom,

$$\{a\} \cup \{b, c\} = \{a, b, c\}$$

2 More Basic Axioms of ZFC and Common Operations

2.1 More Basic Axioms

We will provide two more axioms today, the Subset Axiom and Union Axiom. These will allow us to carry out many of the basic operations of set theory that we know and love. Eventually these axioms will be too primitive to express the kinds of sets we will like to work with and we will add three more axioms, the Axiom of Infinity, the Replacement Axiom, and the Axiom of Regularity.

Remark 2.1. We would like it to be the case such that for any property $P(-)$ of sets, expressible in $\mathscr{L}(\epsilon)$

$$A := \{t : P \text{ is true of t}\}$$

However if we can construct this, we can also construct

$$B := \{t : P \text{ is not true of t}\}$$

If we take the binary union, we can construct the set of all sets

$$\mathbb{V} := A \cup B$$

We will discuss why this creates an inconsistency in a moment. Instead of forming the set of all sets with some property, we can form the set of all sets that are elements of some given set, which have some property.

Remark 2.2 (Informal Subset Axiom (Schema))**.** Informally, for any set X and any property $P(t)$, expressible in $\mathscr{L}(\epsilon)$ there is a set $Y = \{t : t \in X \wedge P \text{ is true of } t\}$

Remark 2.3 (Formulas)**.** How do we construct formulas? We start with the atomic formula, e.g. $z_1 = z_3$, $z_1 \in z_2$. We build up the general formula by applying boolean operations like $\wedge$, $\vee$, $\iff$, $\neg$, $\implies$ and quantification $\exists$ and $\forall$.

Remark 2.4 (Free Variables)**.** Let us begin with an example

$$\varphi = \exists z(x \in y \wedge z = y)$$

In this formula, x and y are free. z is a bound variable, since it is attached to a quantifier. Free variables can actually be plugged into the formula to evaluate the statement. Bound variables are part of the formula.

$$\varphi(x = \{\emptyset\}, y = \{\{\emptyset\}\})$$

This is a true statement. $z = \{\{\emptyset\}\}$ satisfies the formula. Consider the following example

$$x \in x \wedge \exists(x = x)$$

x is both free and bound, since it is free in some instances and bound in other instances.

Axiom 2.1 (Subset Axiom (Schema))**.** *For each formula $\varphi(t, z_1, \cdots, z_n)$ with free variables amongst $t, z_1, \cdots, z_n$ in $\mathscr{L}(\epsilon)$*

$$\forall z_1, \cdots \forall z_n, \forall x \exists y \forall t[t \in y \iff \varphi(t, z_1, \cdots, z_n) \wedge t \in x]]$$

Example 2.1 (Intersection of Sets)**.** $\varphi(t, z_1) : t \in z_1$. Let A and B be two sets. By the subset axiom

$$\exists y \forall t[t \in y \iff (t \in A \wedge t \in B)$$

Thus $y = A \cap B$, so the intersection exists.

Definition 2.1 (Subset Function)**.** We have $(z_1, \cdots, z_n, x) \mapsto \{t \in x : \varphi(t, z_1, \cdots, z_n)\}$

$\Delta_{:\varphi} : \forall z_1, \cdots, \forall z_n \forall x \forall y[y = \{t \in x : \varphi(t, z_1, \cdots, z_n\} \iff \forall t[t \in y \iff (t \in x \wedge \varphi(t, z_1, \cdots, z_n))]]$

Proposition 2.1 (There is no set $\mathbb{V}$ of all sets)**.** *Suppose $\mathbb{V}$ was a set. Then $\forall t(t \in \mathbb{V})$. We can construct, using the subset axiom, the following.*

$$R = \{t : t \notin t\}$$

This is called the Russell Set. We have that $R \in R \iff R \notin R$. Thus no set $\mathbb{V}$ of all sets can exist.

Proposition 2.2 (No universal complement can exist)**.** *Let the universal complement of $\{a\}$, where a is a set, exist.*

$$x = \{t : t \neq a\}$$

Using the b inary union axiom, we can construct $\mathbb{V}$ in the following manner

$$x \cup \{a\} = \mathbb{V}$$

Since such a set cannot exist, we have a contradiction and no universal complement can exist.

Remark 2.5 (On the usage of the Subset Axiom and the Russell Set)**.** Anytime we use set comprehension, we are invoking the Subset Axiom and in doing so we must indicate the parent set from which we are drawing from. Unrestricted comprehension can lead to trouble with the set of all sets. In addition, many of the proofs you will see about whether a particular "universal" set exists will reduce to the construction of the set of all sets. Such a reduction can be useful to keep in your toolbox.

Example 2.2 (Infinite Unions)**.**

$$\bigcup_{n=1}^{\infty} (\frac{1}{n}, 1) = (0, 1)$$

We generalize this to any sequence of sets.

$$t \in \bigcup_{n=1}^{\infty} A_n \iff \exists n(t \in A_n)$$

Further generalizing, we can index by sets instead of the natural numbers.

$$t \in \bigcup_{i \in I} A_i \iff \exists i(i \in I \wedge t \in A_i)$$

Axiom 2.2 (Union Axiom)**.**

$$\forall x \exists y \forall t[t \in Y \iff \exists z(z \in x \wedge t \in z)]$$

Corollary 2.1 (Binary Union Axiom follows from Union Axiom + Pair Set Axiom)**.**

$$A \cup B = \bigcup \{A, B\}$$

$$t \in A \cup B \iff t \in A \vee t \in B \iff \exists z[t \in Z \wedge z \in \{A, B\}] \iff t \in \bigcup \{A, B\}$$

We can construct the binary union operation by using the Union Axiom and the Pair Set Axiom.

Which axioms do we have so far?

- Extensionality
- Pairing
- Power Set
- Empty Set
- Subset Axiom Schema
- Union

2.2 The Algebra of Sets

Fix X. Consider $A, B \subseteq X$

$$A \cup B \subseteq X$$

$$A \cap B \subseteq X$$

$$X \setminus A = A^c = \{t \in X : t \notin A\}$$

We can express all of these operations given the axioms

Proposition 2.3 $(A \cap (B \cup C) = (A \cap B) \cup (A \cap C))$**.**

Proof. $\forall t (t \in A \cap (B \cup C))$
$\iff t \in A \wedge t \in B \cup C$
$\iff t \in A (t \in B \vee t \in C)$
$\iff (t \in A \wedge t \in B) \vee (t \in A \wedge t \in C)$
$\iff t \in A \cap B \vee t \in A \cap C$
$\iff t \in (A \cap B) \cup (t \in A \cap C)$ $\square$

More algebraic facts

$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cup \emptyset = A$$

$$A \cap \emptyset = \emptyset$$

$$A \cap X = A$$

$$(\mathcal{P}(X), \cap, \cup, X \setminus, \emptyset, X)$$

3 Functions and Relations

3.1 Constructing Relations

We will talk about ordered pairs, relations and set up functions today. We would like some way to represent an ordered pair of sets by use of some third set that encodes the pair in an unambiguous, precise manner.

Remark 3.1 (Discussion of Ordered Pairs)**.** We want a construction that takes two sets, a, b and returns a third set $\langle a, b\rangle$ such that for a, b, c, d

$$\langle a, b\rangle = \langle c, d\rangle \implies a = c \wedge b = d$$

Definition 3.1 (Ordered Pair)**.**

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}$$

Proposition 3.1 (Correctness of the construction)**.**

$$\langle a, b\rangle = \langle c, d\rangle \implies a = c \wedge b = d$$

Proof. Case 1: $\{a\} = \{c\}$ and $\{a, b\} = \{c, d\}$.
Thus $a = c$, so $\{a, b\} = \{a, d\}$, implying $b = d$.

Case 2: $\{a\} = \{c, d\}$ and $\{a, b\} = \{c\}$
The first equality gives us that $a = c = d$. Plugging this into the second equality gives us $\{a, b\} = \{c, b\} = \{c\}$, implying $a = b = c = d$

Case 3: $\{a\} = \{c\}$ and $\{b, d\} = \{c\}$. The second equality implies that $b = d = c$, while the first implies $a = c$, which in total means that $a = b = c = d$. □

Proposition 3.2.

$$\forall A \forall a[a \in A \implies \{a\} \in \mathcal{P}(A)]$$

Proof.

$$\{a\} \in \mathcal{P}(A) \iff \{a\} \subseteq A \iff \forall[t \in \{a\} \implies t \in A] \iff a \in A$$

□

Remark 3.2 (Unofficial Cartesian Products)**.** Once we have ordered pairs, now we would like to construct Cartesian Products, as these are fundamental objects in mathematics.

$$A \times B \text{ “=” } \{t : \exists a \exists b, a \in A, b \in B, t = \langle a, b\rangle\}$$

We use the quotation marks, since this is an unrestricted comprehension. To properly use the comprehension (subset) axiom, we need to find which set the elements of $A \times B$ might lie in.
If $t = \langle a, b\rangle = \{\{a\}, \{a, b\}\}$, where $a \in A$ and $b \in B$.
Where does $\{a\}$ belong to? $\{a\} \in \mathcal{P}(A)$. We know $\{a, b\} \in \mathcal{P}(A \cup B)$. Similarly, since $\{a\} \subseteq A \cup B$, we know that $\{a\} \in \mathcal{P}(A \cup B)$. Since the elements of t are elements of $\mathcal{P}(A \cup B)$, we have that $t \in \mathcal{P}(\mathcal{P}(A \cup B))$.

$$\forall t[[\exists a \exists b, a \in A, b \in B, t = \langle a, b\rangle] \implies t \in \mathcal{P}\mathcal{P}(A \cup B)]$$

Definition 3.2 (Cartesian Products)**.**

$$A \times B := \{t \in \mathcal{P}\mathcal{P}(A \cup B) : \exists a \exists b, a \in A, b \in B, t = \langle a, b\rangle\}$$

Remark 3.3 (Examples of Relations)**.** In this class, a relation will typically be a binary relation. Some examples include inequality($a \neq b, a < b$), existence ($a \in b$), subset $a \subset B$, equality $a = b$. In this class, many of these will be relations, since relations must be sets and we cannot have sets the size of the whole universe.

Definition 3.3 (Relation)**.** A relation R is a set such that $\forall t \in R$, there exists sets a and b such that $t = \langle a, b\rangle$.

$$\text{“}aRb\text{”} \implies \langle a, b\rangle \in R$$

Definition 3.4 (Domain)**.**

$$a \in \mathrm{dom}R \iff \exists b \langle a, b\rangle \in R$$

$$\mathrm{dom}R := \{a \in \bigcup \bigcup R : \exists b, \langle a, b\rangle \in R\}$$

Definition 3.5 (Range)**.**

$$b \in \mathrm{ran}R \iff \exists a \langle a, b\rangle \in R$$

$$\mathrm{ran}R := \{b \in \bigcup \bigcup R : \exists a, \langle a, b\rangle \in R\}$$

Definition 3.6 (Field)**.**

$$\mathrm{fld}R := \mathrm{dom}R \cup \mathrm{ran}R$$

Proposition 3.3. *R is a relation $\iff$ $R \subseteq domR \times ranR$*

Proof. $\implies$: $\forall t \in R$,$t \in \mathrm{dom}R \times \mathrm{ran}R$
$\impliedby$: Suppose $\forall t \in R$, $t \in \mathrm{dom}R \times \mathrm{ran}R$. Then $\forall t \in R \exists a \in \mathrm{dom}R, \exists b \in \mathrm{ran}R$ such that $t = \langle a, b\rangle$. Thus every element of R is an ordered pair, so R is a relation. $\square$

Definition 3.7 (Function)**.** A function F is a relation such that

$$\forall a \forall b \forall c[\langle a, b\rangle \in F \wedge \langle a, c\rangle \in F \implies b = c]$$

$$F : X \to Y :\iff F \text{ is a function} \wedge \mathrm{dom}F = X \wedge \mathrm{ran}F \subseteq Y$$

4 More on Relations and Functions

Example 4.1 (Function Example)**.**

$$F : \mathbb{R} \to \mathbb{R}$$

$$x \mapsto x^2$$

$$F = \{t \in \mathbb{R} \times \mathbb{R} : \exists x, x \in R, t = \langle x, x^2 \rangle\}$$

$$\text{ran}F = \{x \in \mathbb{R} : x \geq 0\}$$

Let R, S, A be sets.

Definition 4.1 (Converse Relation)**.**

$$R^{-1} := \{t \in \text{ran}R \times \text{dom}R : \exists a \exists b \exists t, t = \langle b, a \rangle, \langle a, b \rangle \in R\}$$

Essentially, in our (relation) set, we swap every pair of ordered pairs. This should be like an inverse, with the operation of composition.

Definition 4.2 (Composition of relations)**.**

$$R \circ S := \{\langle a, c \rangle : \exists \langle a, b \rangle \in S, \exists \langle b, c \rangle \in R\}$$

$$R \circ S := \{t \in \text{dom}S \times \text{ran}R : \exists a \exists b \exists c, t = \langle a, c \rangle, \langle a, b \rangle \in S, \langle b, c \rangle \in R\}$$

We want this to work similarly to how we think of function composition.

Proposition 4.1. *If F, G are functions, then so is $F \circ G$.*

Proof. Every composition is a relation by definition, so $F \circ G$ is a relation. Let $\langle a, b \rangle \in F \circ G$. Similarly, let $\langle a, c \rangle \in F \circ G$. Unraveling the definitions gives us the existence of some d, e such that $\langle a, d \rangle \in G$ and $\langle d, b \rangle \in F$, as well as $\langle a, e \rangle \in G$, and $\langle e, d \rangle \in F$. Since G is a function, $d = e$. Thus $\langle d, b \rangle \in F$ and $\langle e, c \rangle = \langle d, c \rangle \in F$. Since F is a function, we have that $b = c$. This concludes the proof. $\square$

Remark 4.1 (What is $\text{dom}(F \circ G)$?)**.**

$$\text{dom}(F \circ G) = \{t \in \text{dom}G : \exists c, \langle t, c \rangle \in F \circ G\}$$

$$\text{dom}(F \circ G) = \{t \in \text{dom}G : \exists b \exists c, \langle t, b \rangle \in G \land \langle b, c \rangle \in F\}$$

Definition 4.3 (Relation/Function Restriction)**.** If we want to restrict R to A, we denote this as $R \upharpoonright A$

$$R \upharpoonright A = \{t \in R : \exists a \exists b, a \in A, t = \langle a, b \rangle, t \in R\}$$

We just want to make sure the first coordinate comes from A.

Definition 4.4 (Image of a function/relation)**.** The image of A under R is denoted as

$$R[\![A]\!] = \operatorname{ran}(R \restriction A)$$

Definition 4.5 (Function Application)**.**

$$f(a) = b \iff f \text{ is a function} \wedge \langle a, b\rangle \in f$$

Remark 4.2. We reserve the parentheses notation only for the latter notation. If we wrote $R(A)$, this would indicate that the set A is an element of the domain of R. In the bracket notation, we want to think of A as a subset of the domain of R. This extends the way we think about a function to something on the powerset.

Definition 4.6 (Preimage)**.** We take a look everything in some set which might be in the codomain and we look at every set which maps to this set. The preimage of a set A under R is

$$\{t : a \in A \wedge \langle t, a\rangle \in R\}$$

We can formally write this as

$$R^{-1}[\![A]\!]$$

Proposition 4.2.

$$domR \restriction A = (domR) \cap A$$

Proposition 4.3.

$$dom(R \circ S) = S^{-1}[\![domR]\!]$$

Proof.

$$a \in \operatorname{dom}(R \circ S) \iff$$
$$\exists c, \langle a, c\rangle \in R \circ S \iff$$
$$\exists b, \langle a, b\rangle \in S \wedge \langle b, c\rangle \in R \iff$$
$$\exists b, b \in \operatorname{dom}R, \langle b, a\rangle \in S^{-1} \iff$$
$$a \in S^{-1}[\![\operatorname{dom}R]\!]$$

□

Remark 4.3. We keep using the inverse notation, but the inverse doesn't mean much without an identity. So what is the identity supposed to do? It should take any element $x \in X$ and return x.

Definition 4.7 (Identity Function)**.** For any set X,

$$I_X = \{t \in X \times X : \exists x, x \in X, t = \langle x, x\rangle\}$$

Example 4.2 (Identity Function on the Empty Set)**.**

$$I_\emptyset = \emptyset$$

$$\text{dom}\emptyset = \text{ran}\emptyset = \emptyset$$

$$\emptyset^{-1} = \emptyset$$

Proposition 4.4 (Composition of relation and its converse)**.** *What will $R^{-1} \circ R$ be? Will it be I_{domR}? We know $I_{domR} \subseteq R^{-1} \circ R$*

Proof.

$$t \in I_{\text{dom}R} \iff$$

$$\exists b, b \in \text{dom}R \wedge t = \langle b, b \rangle$$

Since $\exists a$ such that $\langle b, a \rangle \in R$ and $\langle b, a \rangle \in R^{-1}$. Then by definition, $\langle b, b \rangle \in R^{-1} \circ R$. $\square$

Example 4.3 ($I_{\text{dom}R} \neq R^{-1} \circ R$)**.** Let X be any set with at least two elements. For example,

$$X = \{\emptyset, \{\emptyset\}\}$$

Consider the function $F = X \times \{b\}$. Computing the converse yields $F^{-1} = \{b\} \times X$.

$$F^{-1} \circ F = \{\langle x, z \rangle : \langle x, y \rangle \in F, \langle y, z \rangle \in F^{-1}\} = X \times X$$

Definition 4.8 (Single Rooted Relations)**.** A relation R is called single rooted iff

$$\forall a \forall b \forall c [\langle a, c \rangle \in R \wedge \langle b, c \rangle \in R \implies a = b]$$

Remark 4.4. A relation R is single rooted $\iff$ R^{-1} is a function

Definition 4.9 (Injective)**.** A function F is injective if F is single-rooted. We also call injective functions one-to-one.

Proposition 4.5. *If R is a single-rooted relation, then*

$$R^{-1} \circ R = I_{domR}$$

Proof. Suppose $\langle a, c \rangle \in R^{-1} \circ R$. Then there exists c such that $\langle a, b \rangle \in R$ and $\langle b, c \rangle \in R^{-1}$. If $\langle b, c \rangle \in R^{-1}$, it follows that $\langle c, b \rangle \in R$. By the definition of single-rooted, $a = c$. Thus $\langle a, c \rangle = \langle a, a \rangle \in I_{\text{dom}R}$. We proved the other inclusion above. $\square$

Theorem 4.1 (1-1 Functions)**.** *Let $F : X \to Y$ be a function. Then TFAE*

- *F is one-to-one*
- *$\exists g, g : Z \to X \wedge g \circ F = I_X$*
- *F^{-1} is a function and $F^{-1} \circ F = I_X$*

5 Functions and the Axiom of Choice

5.1 Functions

Theorem 5.1 (1-1 Functions)**.** *Let $F : X \to Y$ be a function. Then TFAE*

- *F is one-to-one*
- *$\exists g, g : Z \to X \wedge g \circ F = I_X$*
- *F^{-1} is a function and $F^{-1} \circ F = I_X$*

Proof. We have shown 1 implies 3 in the previous lecture. 3 implies 2 is trivial. Let us prove 2 implies 1.
Supppose there exists $g : Z \to X$ such that $g \circ f = I_X$. Let $a, b \in \text{dom} f = X$. Suppose $f(a) = f(b)$. Apply g to both sides, to get $g(f(a)) = a = b = g(f(b))$. □

Definition 5.1 (Onto)**.** A function $f : X \to Y$ is onto Y if and only if $\text{ran} f = Y$. Similarly, if $\exists g : Y \to X$ such that $f \circ g = I_Y$, then f is onto Y.

Proposition 5.1. *Let R be a relation and let R^{-1} be its converse relation. Then*

$$R \circ R^{-1} \supseteq I_{ranR}$$

Proof. Let $t \in I_{\text{ran}R}$. Then $\exists a \in \text{ran}R$ such that $t = \langle a, a\rangle$. Thus $\exists b$ such that $\langle b, a\rangle \in R$. This implies $\langle a, b\rangle \in R^{-1}$. From that we can conclude that $\langle a, a\rangle \in R \circ R^{-1}$ □

Proposition 5.2. *Let $f : X \to Y$ be a one-to-one function. Then*

$$dom(f \circ f^{-1}) = ranf$$

Proof. We have already shown $I_{\text{ran}f} \subseteq f \circ f^{-1}$. Let $b \in \text{ran}f$. Then $\exists a$ such that $\langle a, b\rangle \in f$, so $\langle b, a\rangle \in f^{-1}$. Thus $\langle b, b\rangle \in f \circ f^{-1}$. Thus $b \in \text{dom}(f \circ f^{-1})$.
Let $b \in \text{dom}(f \circ f^{-1})$. Then $\exists c \exists a$ such that $\langle b, c\rangle \in f^{-1}$ and $\langle c, a\rangle \in f$. Then we know that $\langle c, b\rangle \in f$. Thus $b \in \text{ran}f$ □

Proposition 5.3. *If $f : X \to Y$ is a one-to-one function, then $f \circ f^{-1}$ a function and $f \circ f^{-1} = I_{ranf}$.*

Proof. We showed that $f \circ f^{-1} \supseteq I_{\text{ran}f}$ and that $\text{dom}(f \circ f^{-1}) = \text{ran}f$. Let $t \in f \circ f^{-1}$. Then $\exists a \in \text{ran}f$ and $\exists a, c$ such that $t = \langle a, c\rangle$ and $\langle a, b\rangle \in f^{-1}$ and $\langle b, c\rangle \in f$. It follows that $\langle b, a\rangle \in f$. Since f is a function, we have that $a = c$, so $t = \langle a, a\rangle \in I_{\text{ran}f}$. □

Example 5.1.

$$f : \mathbb{C} \to \mathbb{C}$$
$$z \mapsto z^2$$

Does there exists $g : \mathbb{C} \to \mathbb{C}$ such that $f \circ g = I_{\mathbb{C}}$? f^{-1} is not a function. For every complex number z, we can write $z = re^{i\theta}$ for $r \geq 0$ and $0 \leq \theta \leq 2\pi$.

$$g(z) = \sqrt{r}e^{i\frac{\theta}{2}}$$

$$f(g(z)) = (\sqrt{r}e^{i\frac{\theta}{2}})^2 = |r|e^{i\theta}$$

5.2 Intro to the Axiom of Choice

Axiom 5.1 (Axiom of Choice)**.** *For every relation R, there exists a function F such that $F \subseteq R$ and dom$F$ = dom$R$.*

Remark 5.1. Start with the relation R. For each $a \in \text{dom}R$.

$$R[\![\{a\}]\!] = \{b : \langle a, b\rangle \in R\} \neq \emptyset$$

"Define" $F(a) = b$ by choosing some $b \in R[\![\{a\}]\!]$.

Theorem 5.2 (Axiom of Choice Implies Right Inverses)**.** *$f : X \to Y$ is onto Y if and only if $\exists g : Y \to X$ such that $f \circ g = I_Y$*

Proof. $\Longleftarrow$ was completed earlier today.
$\Longrightarrow$ By the axiom of choice there exists $g \subseteq f^{-1}$ a function with the same domain, Y. ran$g \subseteq \text{ran}f^{-1} = \text{dom}f = X$. Thus $g : Y \to X$ and $g \subseteq f^{-1}$. We conclude that $\text{dom}(f \circ g) = Y$. We know $f \circ g \subseteq f \circ f^{-1} \subseteq I_Y$. If $t \in f \circ f^{-1}$, then $\exists a \exists b$ such that $\langle a, b\rangle = t \in f \circ f^{-1}$ and $\exists c$ such that $\langle a, c\rangle \in f^{-1}$ and $\langle c, b\rangle \in f$. Thus $a = b$ and $t = \langle a, a\rangle$ Since $\text{dom}(f \circ g) = Y = \text{dom}(I_Y)$ and $f \circ g \subseteq I_Y$, we have that

$$f \circ g = I_Y$$

□

Definition 5.2 (Functions from X to Y)**.**

$${}^{X}Y = \{f \in \mathcal{P}(X \times Y) : f : X \to Y\}$$

Example 5.2. Let Y be any set

$${}^{\emptyset}\emptyset = \{f \in P(\emptyset \times \emptyset) : f : \emptyset \to \emptyset\} = \{\emptyset\}$$

$${}^{\emptyset}Y = \{f \in P(\emptyset \times Y) : f : \emptyset \to Y\} = \{\emptyset\}$$

$${}^{Y}\emptyset = \{f \in P(Y \times \emptyset) : f : Y \to \emptyset\} = \emptyset$$

Example 5.3. Let $X = \{1, 2\}$ and let $Y = \{1, 2, 3\}$ Calculate ${}^XY$ and its cardinality.

Axiom 5.2 (Axiom of Choice formulation 2)**.** *Let I, Y be any set. Denote*

$$\bigtimes_{i \in I} X_i = \{f : f \textit{ is a function such that } domf = I \wedge \forall i \in I, f(i) \in X_i\}$$

The axiom of choice states that for $f : I \to Y$ such that $f(i) \neq \emptyset$ for all $i \in I$.

$$\bigtimes_{i \in I} f(i) \neq \emptyset$$

6 Equivalence Relations

Remark 6.1. The main topic for today is the notion of an equivalence relation. They are used to make sense of calling two things the same when they are not literally equal, for whatever intents and purposes in whatever particular case. Part of the goal of this lecture is to turn equivalence relative to an equivalence relation into literal equality through application of some function.

Definition 6.1 (Equivalence Relation)**.** E will be a relation. E is an equivalence relation (on a set X) if

1. $X = \text{fld}(E)$.
2. E is reflexive. i.e. $\forall a \in X, \langle a, a \rangle \in E$. Equivalently, $I_X \subseteq E$.
3. E should be symmetric. i.e. $\forall a \forall b, \langle a, b \rangle \in E \implies \langle b, a \rangle \in E$. Equivalently, $E^{-1} \subseteq E$.
4. E is a transitive relation. i.e. $\forall a \forall b \forall c, \langle a, b \rangle \in E, \langle b, c \rangle \in E \implies \langle a, c \rangle \in E$. Equivalently, $E \circ E \subseteq E$.

Proposition 6.1. *A relation R is transitive if and only if $R \circ R \subseteq R$.*

Proof. Suppose $R \circ R \subseteq R$. Let $\langle a, b \rangle \in R$ and $\langle b, c \rangle \in R$. We know that by the definition of composition, $\langle a, c \rangle \in R \circ R \subseteq R$.
$\Longleftarrow$. Suppose $\langle a, b \rangle \in R$ and $\langle b, c \rangle \in R$. Then we know by transitivity of the relation that $\langle a, c \rangle \in R$. Suppose $\langle a, c \rangle \in R \circ R$. Then there exists a, b, c such that $\langle a, b \rangle \in R$ and $\langle b, c \rangle \in R$. By transitivity, $\langle a, c \rangle \in R$. $\square$

Proposition 6.2. *A relation R is reflexive iff $I_X \subseteq R$, where $X = \mathit{fld}(R)$*

Proposition 6.3. *A relation R is symmetric iff $R^{-1} \subseteq R$ ($R^{-1} = R$)*

Example 6.1. X is the set of formulas in some language.

$$R = \{\langle \psi, \varphi \rangle : \psi \vdash \varphi\}$$

This is reflexive and transitive, but not symmetric.

Example 6.2. Let X be any set.

$$R = I_X$$

This is an equivalence relation.

Example 6.3. Let $X = \mathbb{Z}$. Fix $n \in \mathbb{Z}_+$

$$E_n = \{\langle a, b \rangle \in \mathbb{Z} \times \mathbb{Z} : n|(a - b)\}$$

This is an equivalence relation. Feel free to do the computation to check.

Proposition 6.4. *Let $f : X \to Y$.*

$$E_f = \{\langle a, b\rangle \in X \times X : f(a) = f(b)\}$$

is an equivalence relation.

Proof. Consider $a \in X$. Then $f(a) = f(a)$, so $\langle a, a\rangle \in E_f$. Let $b \in X$ be such that $\langle a, b\rangle \in E_f$. Then $f(a) = f(b) \implies f(b) = f(a)$, so $\langle b, a\rangle \in E_f$. Finally, let $\langle a, b\rangle \in E_f$ and let $\langle b, c\rangle \in E_f$. Then $f(a) = f(b)$ and $f(b) = f(c)$, so $f(a) = f(c) \implies \langle a, c\rangle \in E_f$. $\square$

Example 6.4. Consider the above example

$$E_n = \{\langle a, b\rangle \in \mathbb{Z} \times \mathbb{Z} : n|(a - b)\}$$

$$\text{rem}_n : \mathbb{Z} \to Z$$

$$m \mapsto m\%n$$

$$E_{\text{rem}_n} = E_n$$

Definition 6.2 (E-equivalence Class)**.** The E-equivalence class of $x \in X$ is

$$[x]_E = \{y \in X : \langle x, y\rangle \in E\}$$

Proposition 6.5. *We will construct $f : X \to \mathcal{P}(X)$*

$$f := \{t \in X \times \mathcal{P}(X) : \exists x \exists A, x \in X, A \in \mathcal{P}(X), t = \langle x, A\rangle, A = \{y \in X : \langle x, y\rangle \in E\}\}$$

Claim:

$$E = E_f$$

Proof. Let $\langle a, b\rangle \in E$. Consider

$$f(a) = \{y \in X : \langle a, y\rangle \in E\}$$

$$f(b) = \{y \in X : \langle b, y\rangle \in E\}$$

Consider $y \in f(a)$. Then $\langle a, y\rangle \in E$. Since $\langle a, b\rangle \in E$, by symmetry we have that $\langle b, a\rangle \in E$. By transitivity, $\langle b, y\rangle \in E$, so $y \in f(b)$. Thus $f(a) \subseteq f(b)$. By similar logic, we can show that $f(b) \subseteq f(a)$. Thus

$$f(a) = f(b) \implies \langle a, b\rangle \in E_f$$

$\impliedby$ Let $\langle a, b\rangle \in E_f$. $f(a) = f(b)$. Let $y \in f(a)$. Then $\langle a, y\rangle \in E$. We also know that $y \in f(b)$. Then $\langle b, y\rangle \in E$. By symmetry, $\langle y, b\rangle \in E$. Thus by transitivity, $\langle a, b\rangle \in E$. Thus $E_f \subseteq E$ $\square$

Proposition 6.6.

$$domf = X$$

Proof. Let $x \in X$. $A = \{y \in X : \langle x, y\rangle \in E\}$. Then $\langle x, A\rangle \in t$. Thus

$$X \subseteq \text{dom} f \subseteq X$$

$\square$

Proposition 6.7. *f is a function*

Proof. Let $x \in X$. Consider $\langle x, A\rangle \in f$ and $\langle x, B\rangle \in f$. Then

$$A = \{y \in X : \langle x, y\rangle \in E\}$$

$$B = \{z \in X : \langle x, z\rangle \in E\}$$

By extensionality, clearly $A = B$. $\square$

Remark 6.2. We started with E, an equivalence relation on a set X and constructed

$$f : X \to \mathcal{P}(X)$$

$$a \mapsto \text{E-equivalence class of } a = \{y \in X : \langle a, y\rangle \in E\}$$

We showed that $E = E_f$. A question we might ask is what is the range of f?

Definition 6.3 (Quotients)**.**

$$X/E = \{A \in P(X) : \exists a, a \in X, A = \{y \in X : \langle a, y\rangle \in E\}\}$$

$$X/E = \text{ran} f$$

This is the set of E-equivalence classes.

Definition 6.4 (Canonical Mapping)**.** We will change notation to

$$\pi_E : X \to X/E$$

$$a \mapsto [a]_E = \{y \in X : \langle a, y\rangle \in E\}$$

This is called the canonical mapping