Elements of Algebraic Structures January 12 2024

Lecture 2: Functions, Cardinality and Equivalence relations

Lecture: Sujata Ghosh *Scribe: Aranya Kumar Bal, Sandeep Chatterjee*

1 Topics for this lecture

In this lecture, we shall talk about the following

1. Different types of functions
2. Cardinality of sets
3. Equivalence relations

2 Different types of functions

In what follows, unless otherwise stated, by a relation, we will mean a binary relation.

Let A and B be two non-empty sets and $f : A \to B$.

1. f is well-defined:

A map $f : A \to B$ is called *well-defined* if $a = b$ implies $f(a) = f(b)$ for all $a, b \in A$.

This is really a condition for being a function itself, but we will later see that for maps we define, we would need to verify this to conclude it's a function.
This is really a prerequisite for being a function, but later we will see that this will have uses.

2. f is injective:

A map $f : A \to B$ is called *injective* if $f(a) = f(b)$ implies $a = b$ for all $a, b \in A$. Such a function is also called one-one. It is sometimes denoted as $f : A \hookrightarrow B$, reason being that an injective maps mean that two elements are not mapped to the same element, thus a 'copy' of A is inside B.

Example *Somee examples of injective functions*

- $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 2$
- $f : A \to A$, $x \mapsto x$ *(for any set A)*

3. f is surjective:

For all $b \in B$, there exists some $a \in A$ such that $f(a) = b$. Such a function is also called onto. It is sometimes denoted as $f : A \twoheadrightarrow B$.

Example *Both of the above examples are surjective as well.*

4. f is bijective:

f is both injective and surjective.

$$\forall x, y \in A : f(x) = f(y) \implies x = y \quad \text{and} \quad \forall b \in B, \exists a \in A : f(a) = b$$

More examples:

- $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ is both surjective and injective, hence bijective.
- $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x^2$ is neither surjective nor injective.
- $f : \mathbb{N} \to \mathbb{N}$, $x \mapsto x^2$ is injective but not surjective, hence not bijective.
- $f : \mathbb{R} \to \mathbb{N}$, $x \mapsto x^2$ is surjective but not injective, hence not bijective.

Exercise* Verify all the above examples in 2,3 and 4.

3 Cardinality of a set

We now turn ourselves towards *counting* how many things a set contains. We let $\mathbb{N}_1 := \mathbb{N} \setminus \{0\}$.

We also define a very particular set for simplicity

Definition 3.1 *Let us define the set I_n recursively:*

$$I_1 = \{1\}$$

$$I_{n+1} = I_n \cup \{n + 1\}$$

Definition 3.2 (Finite sets) *A set A is said to be finite if A is empty or there is a bijection $f : A \to I_n$, for some $n \in \mathbb{N}_1$.*

Example *Consider the set $A = \{2, 4, 6, 8, 10\}$. This set is finite because*

$$f : A \to I_5$$
$$x \mapsto x/2$$

is a bijection.

Definition 3.4 (Infinite sets) *A set A is said to be infinite if it is not finite.*

> **Exercise** Show that $\mathbb{N}$ is infinite.

$\mathbb{N}$ being infinite is also intimately tied with an axiom that defines the natural numbers, which can in fact be used as a proof technique.

3.1 Induction and well ordering

Let us introduce the axiom and proof technique here and show a nice property of it. This technique will be very frequently used in this course.

Definition 3.5 (Axiom/Principle of induction) *Let $S \subseteq \mathbb{N}$ such that the following holds:*

1. $0 \in S$
2. *If $n \in S$, then $n + 1 \in S$.*

Then $S = \mathbb{N}$.

This is an axiom (actually a schema) in Peano arithmetic so this cannot be proven from other axioms in Peano arithmetic. But something outside it can provide a proof for it (although that does not make induction any more correct, it just means that whatever axiom set contains that other result is stronger than induction in some sense).

What is this result? It's very intuitive, but first a couple of definitions. We will also rehash a definition from Lecture 1.

Definition 3.6 (Orders) *A partial order on a set X is a relation $\leq$ (written collectively as $(X, \leq)$) is defined as a relation that is reflexive, transitive and antisymmetric.*

A total order on a set X is a partial order with the extra condition that for all $x, y \in X$, either $x \leq y$ or $y \leq x$.

A well order on a set X is a total order such that any non-empty subset of X has a least element (An element $x \in X$ is called least with respect to a total order $\leq$ if for all $y \in X$, $x \leq y$).

> **Exercise*** Show that $(\mathbb{N}, \leq)$ where $\leq$ is the usual ordering on $\mathbb{N}$ is a total order.

Definition 3.7 (Well ordering principle) $(\mathbb{N}, \leq)$ *is a well order.*

Now for the theorem.

Theorem 3.8 *The following are equivalent:*

1. *The well-ordering principle.*

2. The axiom of induction.

Proof. ($2 \Rightarrow 1$) Let us assume 2. Suppose 1 does not hold. Then there is a non-empty subset S of $\mathbb{N}$ such that it does not have a least element.

Let us consider $P(n)$ to be the property that $x \notin S$ for all $x \leq n, x \in \mathbb{N}$. Now since $0 \notin S$ (because if so, then S has a least element, namely 0) and thus $P(0)$ holds.

Assume, $P(k)$ holds for $k \in \mathbb{N}$. Now, if $P(k+1)$ does not hold, then $k+1 \in S$ and $x \notin S$ for all $x \leq k$ and thus S will have a least element (namely $k+1$). Thus $P(k+1)$ also holds.

Then by our assumption, $P(n)$ holds for all n. Thus S is empty which is a contradiction. Thus 1 holds and we are done.

($1 \Rightarrow 2$) Conversely, suppose well ordering principle holds. Let S subset $\mathbb{N}$ satisfying the conditions:

1. $0 \in S$
2. $n \in S$ implies $n + 1 \in S$

We need to show that prove $S = \mathbb{N}$.

Suppose not. Then $\mathbb{N} \setminus S \neq \varnothing$.
Then, well ordering principle tells us that $\mathbb{N} \setminus S = S^c$ has a least element, say k. Now $k \neq 0$ as $0 \in S$.

Is $k - 1 \in S$? Well if not, then $k - 1 \in S^c$, but then k is not the least element of S^c, and thus $k - 1 \in S$.

The by the way we defined S, $(k - 1) + 1 \in S$, that is, $k \in S$ which is a contradiction. Thus $S^c = \varnothing$ and hence $S = \mathbb{N}$.

□

Induction also comes in another flavor, called strong induction.

Definition 3.9 (Principle of strong induction) *Let $S \subseteq \mathbb{N}$, satisfying the following conditions:*

1. $0 \in S$

2. If $k \in S$ for all $k \leq n$, then $n + 1 \in S$.

Then $S = \mathbb{N}$.

Exercise Show that induction and strong induction are equivalent.

How to write 'Proof by Induction'

Given a statement that is *parametrized* by the natural numbers, we can prove it with the help of induction or strong induction whichever is easier.

1. Basic step: We prove the result for the least possible natural number n_0 that is relevant for the statement.

2. Induction Hypothesis: We assume that the statement holds for $n = k$.

3. Induction Step: We prove that the statement holds for $n = k + 1$.

Then the statement holds for all natural numbers $n \geq n_0$.

Exercise Show that $\mathbb{N}$ is infinite using induction.

Here are some other examples infinite sets:
$\mathbb{Z}$: the set of integers
$\mathbb{Q}$: the set of rationals
$\mathbb{R}$: the set of reals

Exercise Show that the above sets are indeed infinite.

3.2 A finer look at cardinality

Consider a set A that is in bijection with some I_n. It makes sense to say that A has n elements. Can we extend this idea to infinite sets? More concretely, we try to answer the following questions.

1. Is it possible to formally define the notion of 'number of elements' of an infinite set?

2. Can we distinguish two infinite sets in terms of the 'number of elements' present in those sets?

Let us now try to answer these questions.

Definition 3.10 (Equipotent sets) *Two sets A and B are said to be equipotent if there is a bijection between A and B.*

Let us define a relation $\sim\sim$ on the collection of all sets such that $A \sim\sim B$ if A and B are equipotent.

Exercise Show that $\sim\sim$ is an equivalence relation.

What is the above equivalence relation on?

I will rehash what we wrote just above

Let us define a relation $\sim\sim$ on the collection of all sets...

Relation on the *collection of all sets*? All your alarm bells should be going off right now, because as we have seen in Lecture 1, the collection of all sets is not a set, and we only know how to define relations on only sets! What is going on?

It's not that big of a deal for us because we are not getting into the nitty-gritty of foundations, but this is a serious problem because such equivalence relations are not really *defined*. We don't know yet how to put a relation structure on proper classes.

But, we can actually do it in a very roundabout manner. We reduce a formula that includes classes to a standard set theory formula syntactically. For example, if we write $S = \{A \mid A \in A\}$, then we know that this is not a set but we can write it as $\forall A (A \in S \leftrightarrow A \in A)$. This is a valid formula in (ZF) set theory but does not define anything in the theory itself (in the meta-language, we know this is a class but that's about it).

In general, a class $\mathbf{C}$ is syntactically written as a formula φ, which is short hand for $x \in \mathbf{C} \leftrightarrow \varphi(x)$. We can use this to define relations on classes. I don't mention how exactly one does that, but it can be done. The upshot of all the hardwork? Nothing very interesting happens : Relations look the same for classes as they do for sets. Just one of those things.

But what does come out is something called [Scott's trick] (which was possibly first demonstrated with regard to equipotent sets, so it's pretty relevant here). Scott's trick (is really a trick that) allows you to bypass the problem of the equivalence classes being proper classes and pluck a representative from them. If they are proper classes, we can't directly do that because, well, classes are not defined in ZF. Scott's trick is a little hard to explain here, again because we lack several prerequisites, but again this can be done. In fact, it gives us the aleph numbers without choice!

I will leave this at this point, there are several keywords here one canlook up if one wants.

Properties of equivalence relations

Equivalence relations have been brought up in our discussion from time to time, and they are one of the core principles of doing mathematics. Why are they so important is due to one of the most beautiful *structural* property of such relations. Let's build towards that.

Definition 3.11 (Classes of a relation) *Let $\sim$ be a relation on A. Then we define the left class of $a \in A$ as the set*

$$[a]_L := \{b \mid b \sim a\}$$

The right equivalence class of a is similarly defined

$$[a]_R := \{b \mid a \sim b\}$$

Proposition 3.12 *If a relation is symmetric, then $[a]_L = [a]_R$ for all $a \in A$.*

Proof. Let $x \in [a]_L$. Then $x \sim a$. By symmetricity $a \sim x$ which implies that $x \in [a]_R$. Thus $[a]_L \subseteq [a]_R$ Running the argument in reverse, we get $[a]_R \subseteq [a]_L$. Thus $[a]_L = [a]_R$. □

Thus if a relation is symmetric, we can talk just about an element's class $[a]$, rather than the left and right classes separately. If the relation is an equivalence relation, we call these classes *equivalence classes.* The set of equivalence classes is written as $A/\sim$.

Couple more definitions before we can state the result.

Definition 3.13 (Partion of a set) *Let A be a set. A collection of sets $\{A_i\}_{i \in \mathcal{I}}$ is called a partition of A if*

1. $A_i \subseteq A$ *for all* $i \in \mathcal{I}$
2. $A_i \neq \varnothing$ *for all* $i \in \mathcal{I}$
3. $A_i \cup A_j = \varnothing$ *for all* $i, j \in \mathcal{I}$
4. $\bigcup_{i \in \mathcal{I}} A_i = A$

If such a thing happens, then we say that $\{A_i\}_{i \in \mathcal{I}}$ partitions A.

Now the crux, the main theorem. This should really be given the name as some fundamental theorem, or at least called the band-aid theorem (for reasons that I might put in a box later).

Theorem 3.14 *Let A be a set with an equivalence relation $\sim$. Then the equivalence classes of $\sim$ partition A. Conversely, if there is a partition of A, then there is an equivalence relation on A such that the equivalence classes agree with the partitions.*

Exercise Prove the theorem.

The exercise is really just a check in the forward direction and requires just a little thinking in the other direction. It's a very important theorem, yet has a very simple proof!

Band-aid theorem

The above theorem tells us that equivalence relation and partitions are the same thing. But why is this useful? And why did I call it *band-aid* theorem?

Let us look at a real life example first. Suppose you have bought some fruits and now you want to understand what fruits you have bought. You are not really interested in the number of fruits you have bought. So you define two fruits to be related if they are of the same type. This partitions the set of all fruits you bought into respective categories, say apples, oranges and mangoes. So instead of looking at the fruits thmselves, you take a step back and look at the categories of fruits and they give you an answer.

This oftentimes happen in maths. Sometimes, the object you are looking at has too much detail in it which you don't really bother about. You take a step back and bunch some of the details together to look at details that were not visible at a higher resolution. Like zooming out. Equivalence relations are the way you do this.

As a very concrete example (this comes in a first class in algebraic topology and thus might be a little *out there*, so feel free to skip this), consider how we define the fundamental group of a pointed topological space (X, x_0). we consider the set of all loops based at x_0, and an operation of loop concatenation (basically, if two loops are concatenated, you go around the first loop, then go around the second loop). This has too much detail in it, like two loops are the same if they are literally the same loop etc. This does not let us do a whole lot. But if we take a step back and consider two loops as related if one can be *continuously transformed* into the other,which by the way is an equivalence relation, then we get something astonishing. The equivalence classes form a group under concatenation!

And this repeats in several places. You have some object and you use a band-aid of some equivalence relation to get a better object.

It even acts as a band-aid, or well, more like a glue in a completely different context! Consider you have two sets X and Y. Now you want to *glue* X and Y together along subsets $A \subseteq X$ and $B \subseteq Y$. So what you do is, you apply glue to A and B and stick them together; mathematically, you consider the set $X \sqcup Y$ (this is the [disjoint union] of the sets) and define a relation $\sim$ on this such that $a \sim b$ if $a, b \in A \sqcup B$ (which is basically saying that these are all the points getting glued). The set of equivalence classes $(X \sqcup Y)/\sim$ is exactly what your glued space looks like.

This gluing is absolutely essential when we study graphs and topological spaces and other geometric objects!