studies-in-algebra-and-group-theory
XXXX – Harvard University

S. D. V. Stephens

October 13, 2025

Contents

Lecture 1.

Naïve-set-theory

1.1 Ordered Pairs

We begin with a discussion of ordered pairs. Consider a set of numbers $\{1,2,3,4\}$. For any set there is no particular order that triumphs over another, i.e., $\{1,2,3,4\} = \{1,3,2,4\} = \{3,4,2,1\} = \ldots$, an obvious truth. Say we want $\{1,2,3,4\}$ to be in the order of $\{3,2,1,4\}$ for some arbitrary reason; we may then consider the collection,

$$\mathscr{C} = \{\{3\},\{3,2\},\{3,2,1\},\{3,2,1,4\}\}.$$

It becomes obvious what is happening here: the method by which we get order is dependent on the number of iterations in which a particular element appears in any number of sets in a given collection (in comparison to the other elements in the other sets of the respective collection).

Then consider this process but for a nested collection (a collection within a collection) which contains two sets, namely the arbitrary elements a,b in opposing orders, and notice that it gives us the definition of a 2-tuple (ordered pair),

$$\mathscr{C}_1 = \{\{a\},\{a,b\}\} \coloneqq (a,b) \text{ and } \mathscr{C}_2 = \{\{b\},\{b,a\}\} \coloneqq (b,a).$$

Note:-

This form of generating or representing ordered pairs is called the *Kuratowski encoding* of ordered pairs.

This, of course, naturally extends to greater n-tuples. There are some obvious consequences of this that will not be gone over here.

The **Cartesian product** is a set of ordered pairs which can be given by taking power sets.

Definition 1.1.1: Cartesian product

The cartesian product is the cross product of two sets given by

$$A \times B = \{(a,b) \mid a \in A, b \in B\}\},$$

where, by the Kuratowski encoding,

$$(a,b) \coloneqq \{\{a\},\{a,b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B)).$$

1.2 Relations

The review or ordered pairs leads us to our next discussion on relations. A relation in more colloquial terms is a dynamic or characteristic of a given element shared with another given element such that they are arranged in the form of ordered pairs. Think of equality, then think of equality as equating $(2+3, 1+4)$, or perhaps something more interesting, the set of all (x,y) such that x is a man, y is an enby (slay), and x is married to y (many such cases). We can then think of relations as a set of ordered pairs $R \subset A \times B$. Consider the following examples:

1. $R \coloneqq \{(x,y) \in \mathbb{N}^2 \mid y - x > 0\} \iff xRy \equiv y > x$, the relation of greater than;
2. $R \coloneqq \{(a,B) \in A \times \mathcal{P}(A) \mid a \in B\} \iff aRB \equiv a \in B$, the relation of *belonging* (being an elemnt of);
3. $R \coloneqq \{(c,d) \in \{\text{all cats}\} \times \{\text{all dogs}\} \mid$ c and d live in the same house$\}$.

Naturally, there are an infinite number of possible relations, however there is a particular class of these which we are interested in for the time being—that which relates two equivalent elements (the definition of what equivalence means is, for now, notably ambiguous).

1.2.1 Equivalence relations and partitions

If a relation R exists s.t. xRx for any $x \in X$, then we say R is reflexive. If $xRy \iff yRx$, it is symmetric, and if $xRy,\ yRz \implies xRz$, it is transitive. If a given relation R satisfies all three of these properties (reflixivity, symmetry, transitivity), then we say it is an ***equivalence relation***.

Definition 1.2.1: Equivalence relations

An equivalence relation, usually denoted $\sim$, is a relation that is reflexive, symmetric, and transitive $\forall (a, b) \in A \times B$.

Question 1

Consider each of the three qualifiers (axioms) for the existence of an equivalence relation. Find an explicit relation that has one property but not the other for each of the three axioms.

Solution: I apologize for the terse abstraction involved in this first example, but let

$$R \coloneqq \{(1,1),(2,2),(3,3)(1,2),(2,3) \in \{1,2,3\}^2\},$$

notice that $(1,1),(2,2),(3,3)$ is true for R, thus reflixivity holds; however, it is quick to see that $(1,2)$ exists in R but $(2,1) \notin R$, thus symmetry cannot hold. For transitivity, notice that we have $(1,2)$ and $(2,3)$, so we can set up the first step, but $(1,3) \notin R$! Thus transitivity fails. This example is a reminder that we need not think of concrete properties that can be applied in front of our eyes (shapes, dogs, even equality!) in order to have or manipulate some sort of mathematical relation. Next, consider a the relation $R \coloneqq \{(a,b) \mid a \neq b\}$. First, aRa is categorically untrue thus reflixivity means nothing to us. Symmetry, however, tells us that if aRb then bRa, which is true! Transitivity may seems sneakily true at first, but notice that $aRb,\ bRa \implies aRa$ is not true (we simply replaced c with another instance of a). Finally, transitivity as a singular property is pretty straightforward. Consider $x > y$, notice that $x > x \implies x < x$ is categorically untrue since x can never be greater or less than itself, additionally, $x > y$ never implies $y > x$. For transitivity however, notice that $x > y,\ y > z \implies x > z$ is true!

Next we move onto partitions, and to start we must define them! But first I note that we bring up partitions not onyl for their interestingness but also since they have a direct relation to equivalence relations via something known as *equivalence classes*.

Definition 1.2.2: Partitions

A partition of a set X is a disjoint collection $\mathscr{C}$ (i.e., a collection in which all the sets inside contain no common elements with the other sets inside $\mathscr{C}$) of non-empty subsets whose union is X itself.

Example 1.2.1 (Partitions of $\mathbb{Z}$)

Consider $\mathbb{Z}$. Notice that we can seperate this into a distinct collection of disjoint sets—i.e., we can partition $\mathbb{Z}$—by taking all multiples of a given number, represented by $n\mathbb{Z}$, where each sequential $n\mathbb{Z} + m$ has the property that if any $n\mathbb{Z} + k$ s.t. $k < m$ has the same multiple, it will not inclue said multiple in itself. Explicity this is given by $\mathscr{C} = \{n\mathbb{Z}, n\mathbb{Z}+1, n\mathbb{Z}+2, \ldots\}$ and $\mathbb{Z} = n\mathbb{Z} \sqcup n\mathbb{Z}+1 \sqcup n\mathbb{Z}+2 \sqcup \ldots$

Definition 1.2.3: Equivalence classes

An equivalence class of x with respect to R is the ***class***—which we may use instead of the word "set" for traditional and conventional reasons rather than practical, but for all intents and purposes is the same—of all y such that xRy holds.

Example 1.2.2 (Equivalence classes)

If R is equality in X, then any equivalent class is simply going to be a singleton, and thus the partition of X with respect to R will be entirely comprised of singletons.

Combining equivalence classes and partitions reveals something interesting: the notion of modulos. Since notation is not standard in regards to equivalence classes I'll quickly mention just two—x/R and $[x]_R$ are both examples of "the equivalence class of x with respect to R." For now we will keep with the notation of x/R (for reasons you will see shortly), though when not dealing with modulos I personally prefer $[x]_R$ notation. The set of all equivalnence classes denoted X/R (or $[X]_R$) can be read as X modulo R or simply X mod R (the standard mod you are familiar with).

Question 2

Show that X/R is indeed a set by exhibiting a condition that specifies exactly the subset X/R of the power set $\mathcal{P}(X)$.

Solution: We begin with $\mathcal{P}(X)$, notice that $\mathcal{P}(\mathcal{P}(X))$ contains all possible ordered pairs of X in the form $\{\{a\},\{a,b\}\}$. Thus, we can say that whatever R is, it is a subset of the subset of all possible ordered pairs in $\mathcal{P}(\mathcal{P}(X))$. Also notice that X/R forms a partition of X, and we know that partitions of a set A are subsets of the powerset of A. I must admit however, most of this was simply a reminder as what we must actually do is invoke Aussonderungsaxiom, so,

$$X/R \coloneqq \{S \in \mathcal{P}(X) \mid S \neq \emptyset \text{ and } \exists a \in X : S = [a]_R\}.$$

If we wish to simplify this crude and complicated notation even further we can simply write

$$X/R \coloneqq \{S \in \mathcal{P}(X) \mid \Gamma(S)\},$$

where $\Gamma(S)$ means S is a non-empty equivalence class under R (let not greek letters scare you!).

Returning to our discussion of relations and partitions we can have this thing called an *induced relation*. Let $R \coloneqq X/\mathscr{C}$, we say that if $x, y \in \mathscr{C}$ and $xX/\mathscr{C}y$, then $X/\mathscr{C}$ is the relation *induced* by the partition $\mathscr{C}$.

Proposition 1.2.1 Relationship between equivalence relations, classes, and set partitions

Explicitly the relationship between the two is given as follows: if R is an equivalence relation on X, then the set of equivalence classes form a partition of X that induces the relation R, and if $\mathscr{C}$ is a partition of X, then the induced relation is an equivalence relation whose set of equivalence classes is exactly $\mathscr{C}$.

Proof of Prop. 1.2.1: It is given that the union of $[x]_R, \forall x \in X$ is X itself. Additionally, it quickly follows that if any two equivalence classes $[a]_R, [b]_R$ share an element in common they are the same equivalence class and all their elements are in common, observe: if $z \in [x]_R \cap [y]_R$ then xRz and zRy, thus by transitive property innate to equivalence relations, xRy (and thus they are the same under R). The only possibility then is that each equivalence class must be disjoint and therefore is a partition. Partitions implying equivalence classes is much faster: reflixivity, symmetry, and transitivity are automatically given if $x, y, z \in S \in \mathscr{C}$. □

1.3 Functions

First I want to remind us of some notation and terminology things (mathematicians are ***very*** specific):

Reminder!

To say a function is *on* X *into* Y, means that the function is from X to Y.

Definition 1.3.1: Functions

We all know what functions are at some level, but here were are going to be extraordinarily explicit (though you likely have already heard it in this form, regardless). A function on X into y is a relation (R) given by a letter like $f, g, h, \varphi, \ldots$, such that:

1. $\operatorname{dom} f = X$;
2. if $(x, y) \in f$ and $(x, z) \in f$, then $y = z$ (uniqueness of y for each x); additionally, $f(x) = y$ is conventional notation (insteaf of $(x, y) \in f$ or xfy);
3. y is called the ***value*** that f ***assumes*** at the ***argument*** x; i.e., f ***maps/ sends/ transforms*** x to/ into y. We often use the terms map, mapping, transformation, correspondence, operator, and function interchangably.

We denote this correspondence via

$$f : X \to Y.$$

Finally, we note that the set of all function from X to Y is subset of the power set $\mathcal{P}(X \times Y)$ and is denoted Y^X.

Something to note is that a function is not an active entity despite action-invoking words such as *transforms*; it merely *is*. The use of the word function to describe the undefined object that is somehow active in relation to a graph is nevertheless a static set, similar to that of a directory of names that correspond to addresses. Reminder that while the $\operatorname{dom} f = X$, it need not be the case that $\operatorname{ran} f = Y$, instead the range is reserved for the subset of all $y \in Y$ that have a corresponding x such that $f(x) = y$, i.e., is mapped to by some x. We call this property being ***onto*** and we say f maps X ***onto*** Y; more commonly however we say that f is ***surjective***—we explicitly write this as $\forall y \in Y, \exists x \in X : f(x) = y$—and we denote this surjectivity via

$$f : X \twoheadrightarrow Y,$$

and if $A \subset X$, we may consider all $y \in Y$ such that there is an $x \in A$ such that $f(x_A) = y$ (here I use x_A as crude shorthand for $f(x)$ s.t. $x \in A$, where Halmos uses the more primitive $f(A)$), the set of those $y \in Y$ is known as the ***image*** of f under A. If it is the case that $X \subset Y$, the function f defined by $f(x) = x, \forall x \in X$, we call this the ***inclusion map/ embedding/ injection*** or we say f is ***one-to-one***; we explicitly write this as $\forall a \neq b,\ f(a) \neq f(b)$. We denote injectivity via

$$f : A \hookrightarrow Y.$$

A special case of injectivity comes when we inject $X \hookrightarrow X$, relation-wise this is equality in X, language-wise, we call this the ***identity map*** on X.

Proposition 1.3.1 Restriction and extensions

Consider a function $f : Y \to Z$ and a set $X \subset Y$. We say that there is a *natural way* of constructing a new function $g : X \to Z$; let $g(x) = f(x), \forall x \in X$, we then say g is a ***restriction*** of f to X and f is the ***extension*** of g to Y. We denote this as $g = f|X$ where we can express the definition as $(f|X)(x) = f(x) \forall x \in X$ and $\operatorname{ran}(f|X) = f(x_X)$.

There are a few other terminologies that follow from all that has been mentioned so far, and I will go through them rather quickly:

i. f is called the ***projection*** (pr) from $X \times Y$ onto X if $f(x,y) = x$; similarly if $R = X \times Y$, then instead of being the projection of R onto X, it is now the range of the projection f;

ii. Let R be an equivalence relation in X and $f : X \to X/R$ defined by $f(x) = x/R$; this function is called the ***canonical map*** from X to X/R;

iii. expounding on our notion of inclusion mappings and surjections from earlier, ***bijectivity***—one-to-one correspondence-ness—is a function that is both injective and surjective, and is derived from an equivalence relation R in X with $aRb \iff f(a) = f(b)$ for $a, b \in X$; so given a function/ set $g(y) = \{x \in X \mid f(x) = y, \forall y \in Y\}$, the equivalence relation R tells us that $g(y)$ is an equivalence class of the relation R; that is to say, we define the function as $g : Y \twoheadrightarrow X/R$, notice that for g, if $c \neq d$, $c, d \in Y$, due to the nature of equivalence classes (remember, all the classes are disjoint), $g(c) \neq g(d)$; notice this is the exact explicit definition of injectivity, thus this is a surjective-injective, i.e., bijective mapping. Although there is no universially agreed on notation for bijection, we shall denote this mapping as $g : Y \leftrightarrow X/R$;

iv. finally, we have the notion of a ***characteristic function***. If $A \subset X$ the characteristic function of A is the function $\mathcal{X} : X \to 2$ given by $\mathcal{X}(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \in X - A \end{cases}$, however, we may write $\mathcal{X}_A$ to indicate that it depends on A. The function that assigns to each $A \subset X$, i.e., $\mathcal{P}(X)$, the characteristic function of $A \in 2^X$ is a bijection, i.e., $f : \mathcal{P}(X) \leftrightarrow 2^X$.

Question 3

Concerning bijectivity (point iii.), the examples have all the inclusion maps as one-to-one, however, except in a few trivial special cases, the projections are not. What are these special cases?

Solution: do this in a bit

Question 4

Prove:

a) $Y^{\emptyset}$ has exactly one element, namely $\emptyset$, regardless of if Y is empty or not;

b) if X is non-empty, then $\emptyset^X$ is empty.

Solution:

Proof: a)

□

Note:-

I should note that the time spent on this almost expository writing for these notes has been incredibly time-consuimg and thus, from this point on, things will be cut down and significantly more dense.

1.4 Families

1.5 Inverses and Composites