Math-55a
XXXX – Harvard University

S. D. V. Stephens

October 17, 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., $\{1,2,3,4\} = \{1,3,2,4\} = \{3,4,2,1\} = \dots$, 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),

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

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,

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

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

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 only 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 (instead of $(x, y) \in f$ or $x f y$);
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

$$f : X \longrightarrow Y.$$

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 $f : Y \longrightarrow Z$ and a set $X \subset Y$. We say that there is a *natural way* of constructing a new function $g : X \longrightarrow Z$; 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 universally 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 $A \subset \mathrm{X}$, i.e., $\mathcal{P}(\mathrm{X})$, the characteristic function of $A \in 2^{\mathrm{X}}$ is a bijection, i.e., $f : \mathcal{P}(\mathrm{X}) \leftrightarrow 2^{\mathrm{X}}$.

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: Consider a function's projection as the cannonical map $\gamma : \mathrm{X} \to X/R$, the following cases are trivial examples of non-injective projection maps:

1. $X = \emptyset$, vacuously fulfilled (it matters not what R is);
2. $R := \{(x, x) \mid x \in \mathrm{X}\}$, so every equivalence class is a singleton.

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:

a) ***Proof:*** Given that $Y^{\emptyset} \subset \mathcal{P}(\emptyset \times Y)$, and the definition of Cartesian sets has **and** as a qualifier, i.e., $A \times B = \{(a, b) \mid a \in A \textbf{ AND } b \in B\}$, we can see that $\emptyset \times Y$ contains in fact no elements which satisfy this, and thus, it is the empty set. So $Y^{\emptyset} \subset \mathcal{P}(\emptyset) = \{\emptyset\}$, thus the only element that can be in $Y^{\emptyset}$ is the singleton $\{\emptyset\}$. This is a vacuous satisfaction and is non-intuitive; some intuition, perhaps, may be gained but thinking "*the only thing nothing can map to is nothing*," or by taking the cardinality of these two sets with each other given by $|\emptyset| \cdot |Y| = 0|Y| = 0$ (though this is mainly for intuition). □

b) ***Proof:*** $\emptyset^X$ means that something must map to the emptyset, meaning there must be an element within the emptyset, but this cannot be true! Thus, by definition, the set must be empty. □

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

Forget literally everything you know about notational convention! Why? Idk, that's just how mathematicians decided to approach this topic—the family (*awwwwww*). Consider a function x (yes, this is strange) s.t. $x : I \longrightarrow X$. We call I the ***index set***, and thereby each $i \in I$ is an ***index***; the range of the function is then called the ***indexed set*** (why, this is so stupid?!); the function has a special name, being called a ***family***, and the value of x at a given i is called a ***term*** of the family (denoted x_i). Other even more bewildering notation may be used such as $\{x_i\}$ being a family in X or, more horrificially, a family $\{A_i\}$ of subsets of X, being a function $A : I \longrightarrow \mathcal{P}(X)$ (now that I think of it, this notation, sickeningly, is becoming somewhat preferable).

Given that ran$(\{A_i\} = \bigcup_{i \in I} A_i)$, we notice that every arbitrary collection of sets is in fact the range of some arbitrary family: consider I and X equal to $\mathscr{C}$ s.t. $\{A_i\} : \mathscr{C} \longrightarrow \mathscr{C}$. I am realizing it is the terminology which is so obtuse, that what I do not like.

We may think of $\bigcup_{i \in I} A_i$ as $\bigcup_{i=1}^{n} A_i$ (similar to what we have seen for summations and products), where n is the order of i and we assume 1 is the first element in i.

Example 1.4.1

For some index set $i = \{1, 2, 3\}$, and an indexed set A_i we have $\bigcup_{i=1}^{3} = A_1 \cup A_2 \cup A_3$. Another example may be given as follows: let $I = \mathbb{N}$, and $A_i = \{-i, 0, i\}$, that is to say for every i we have $A_1 = \{-1, 0, 1\}, A_2 = \{-2, 0, 2\}, \ldots$, and so on. Notice that the infinite union of A_i produces $\mathbb{Z}$ and the infinite intersection produces $\{0\}$.

Example 1.4.2

Let us now consider an uncountably infinite indexing set it a plane $I = [-1, 1], A_i = \{i\} \times [0, 1] \subset \mathbb{R}^2$. Notice this is going to be a subset of ordered pairs, i.e., $\{(i, y) \mid 0 \leq y \leq 1\}$. Geometrically, the union over all $i \in I$ of A_i gives us a rectangle in $\mathbb{R}^2$ defined by $[-1, 1] \times [0, 1]$; similarly the intersection of these sets, notice, are intersections of finite parallel lines, thus there exists no element in common with these sets, thus it is $\emptyset$.

Theorem 1.4.1 Associative Law of Unions

Let $\{I_j\} : J \longrightarrow K \mid K = \bigcup_{j \in I}$ and $\{A_k\} : K \longrightarrow X$, then

$$\bigcup_{k \in K} A_k = \bigcup_{j \in J} \left(\bigcup_{i \in I_j} A_i \right).$$

Question 5

Prove the associativity and commutativity of unions.

Proof: Exercise for the reader :) (sorryyyyy) □

Note:-

Regarding notation of indexed sets, it is useful to point out that $\bigcup_{i,j} = \bigcup_{(i,j) \in I \times J}$.

De Morgan's laws apply standardly for index/ indexed sets and their unions. From such, it is easy to see that if $\{A_i\}, \{B_i\}$ are families of sets, then $\bigcup_i A_i \cap \bigcup_j B_j = \bigcup_{i,j}(A_i \cap B_j)$, a similarly for $\bigcap_{i,j}(A_i \cup B_j)$.

Let us consider a special type of family: let $I = \{a, b\}$, $a \neq b$ and let Z be the set of all families z indexed by I such that $z_a \in X, z_b \in Y$. Now consider $f : Z \leftrightarrow X \times Y$ such that $f(z) = (z_a, z_b)$. This is the ***generalized Cartesian product***! There is further detail one can go into about families of sets and sets of all given families of sets, and even sets of those sets (including their Cartesian products), but these are so disgusting as to induce spontanous wretching in even the most tough-stomached mathematicians. So we will avoid it, if possible.

1.5 Inverses and Composites

Consider a function $f : X \to Y$, a natural mapping that might arise (when thinking on power sets) is some function $F : \mathcal{P}(X) \to \mathcal{P}(Y)$; just as each element of X is mapped to an element Y under f, each subset of X maps to some subset of Y under F, so if $A \subset X$ then $\exists(A \mapsto \mathrm{Im}(f_A))\forall A \in \mathcal{P}(X)$. Cool? I guess? What is to be done about this? In all honesty, I am not sure this factoid has much use other than being a pedagogical tool (though I am almost certainly wrong and I am sure someone will rush to correct me, wherein I might toil and languish over my incorrectness and stupidity, suffering immensely—but probably not, because I simply do not care), but for our cases we use it to introduce its behavior in the inverse.

Note:-

Regarding notation—as we all too often are—$\mathrm{Im}(f_A)$ is the same thing as $f(A)$ when regarding images of subsets. I prefer the former notation as it feels a bit more natural to me.

Definition 1.5.1: Inverses and inverse images

Given a function $f : X \to Y$ we say f^{-1} is the ***inverse*** of f given by $f^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$ such that if $B \subset Y$, then

$$\mathrm{Im}(f_B^{-1}) = \{x \in X \mid f(x) \in B\},$$

is the ***inverse image*** of B under f.

This definition results in some immediate necessary and sufficient conditions: first, for $f : X \to Y$ to exist, the inverse image under f of each non-empty subset of Y must be a non-empty subset of X; second, for f to be injective is that the inverse image under f of each singleton in the range of f be a singleton in X.

Note:-

We often use f^{-1} for another purpose: for some $f : X \to Y$, $f^{-1} : \mathrm{ran}(f) \to X \implies f^{-1}(y) = x \iff f(x) = y$. This will be the most common use case for f^{-1} as the inverse function $g : Y \to X$.

There are some connections betwefen images and inverse images which I will quickly enumerate, but I will not provide proof for (for the proofs see Halmos, pp. 59): Let f be a function such that $f : X \to A$ for each of the following,

i. $B \subset Y \implies f(f^{-1}(B)) \subset B$;

ii. $f : X \twoheadrightarrow Y,\ B \subset Y \implies f(f^{-1}(B)) = B$;

iii. $A \subset X \implies A \subset f^{-1}(f(A))$;

iv. $f : X \hookrightarrow Y,\ A \subset X \implies f^{-1}(f(A)) = A$;

v. If $\{B_i\}$ is a family of subsets of Y, then $f^{-1}(\bigcup_{i\in I} B_i) = \bigcup_{i\in I} f^{-1}(B_i)$ and $f^{-1}(\bigcap_{i\in I} B_i) = \bigcap_{i\in I} f^{-1}(B_i)$;

vi. $f^{-1}(Y - B) = X - f^{-1}(B)$ for each $B \subset Y$.

We now move onto ***composites***.

Definition 1.5.2: Composition

Let $f : X \to Y$ and $g : Y \to Z$ it is clear that we can make a map from $X \to Z$ since the range of f can be the domain of g. We can represent this new function—i.e., the ***composite function***—as either $h : X \to Z$ or $g \circ f$, and often simply just gf. We read this right to left.

Notice that function composition is not always commutative, nor need it be. Also notice that this remains true under the special case that $f : X \to Y$ and $g : Y \to X$; functional composition, however, is always associative. There will be a strong proof for this later on (in Groups). Notice that if $g : X \to Y$ for standard f, if it is bijective we have an inverse function and identity map given by h. Functional composition under inverses appears something like this: if $f : X \to Y$ and $g : Y \to Z$, and $f^{-1} : \mathcal{P}(Y) \to X$ and $g^{-1} : \mathcal{P}(Z) \to \mathcal{P}(Y)$. Then $g \circ f$ has an inverse given by $f^{-1} \circ g^{-1}$. Notice this is not true for $g^{-1} \circ f^{-1}$.

1.5.1 Inverse/ converse and composite relations

The main idea of this comes out of our exploration of inverse functions. Functions *are* relations after all. Consider the ***converse relation*** of R on $X \times Y$ s.t. xRy and $yR^{-1}x$. Similar things can be done for composites by generalizing composition to relations, observe: let S be a relation on $Y \times Z$ and R be a relation on $X \times Y$ such that xRy and ySz. Now let T over $X \times Z$ be given by $S \circ R$ such that xTz exists $\iff \exists y \in Y$ such that xRy and ySz. Congrats! You made a ***composite relation***. If it is the case that R and S are functions s.t. $R(x) = y$, $S(y) = z$ and $S(R(x)) = z \iff xTz$ which implies that functional composition is a special case of a greater abstraction called the ***relative product***(??).

Lecture 2.

Groups

2.1 Group basics

Definition 2.1.1: Groups

A ***group*** is a set S together with a map

$$m : S \times S \to S$$

called a ***law of composition*** (LOC) (also called ***binary operation***). Writing ab for $m(a,b)$, the LOC has to satisfy three axioms (known as the group axioms):

i. (existence of identity): $\exists e \in S$ called the *identity* such that $ea = ae = a$, $\forall a \in S$;

ii. (existence of inverse): $\forall a \in S, \exists b$ such that $ab = be - e$ (we often denote b as $-a$ or a^{-1});

iii. (the associative law): $\forall a, b, c \in S$, $a(bc) = (ab)c$.

Now some notes: from the definition it quickly follows that the identity of a group is unique, and this is easy to show. Due to inverses, we have been gifted with the *cancellation law*, $ab = ab' \implies b = b'$. Finally, (S, m) is our pair which constructs our group, however, it is often that we will simply use one letter to denote the group (often G or the same letter used with the underlying set, e.g., S). Instead of using $|G|$ to denote cardinality, we will often use it—in the context of groups—to denote the underlying set; the cardinality of the group/ underlying set, then, too, undergoes a name change—it is known as the *order* of the group.

Note:-

It is customary to use + as the representative operation for commutative laws (i.e., when it is the case that the group is not only associative, but also commutative). This does not, however, imply that multiplication is reserved for non-commutativity.

2.1.1 Group Variants

There are special cases of group-like-structures with more or less group axioms, here we list a few which we will define informally:

Definition 2.1.2: Abelian groups

An abelian group is a group G such that all $a, b \in G$ commute under the law of composition.

Definition 2.1.3: Monoids

A ***monoid*** is an algebraic structure with the same underlying structure as a group (i.e., set and LOC) and two out of three of its axioms—namely missing inverses.

Definition 2.1.4: Semigroup

A ***semigroup*** is an algebraic structure with the same underlying structure as a group (i.e., set and LOC) and two out of three of its axioms—namely missing associativity.

Example 2.1.1

$Z/n := \{0, 1, 2, \ldots, n-1\}$, with a group law given by addition mod n, where

$$m(a,b) := \begin{cases} a+b, & \text{if } a+b \leq n-1 \\ a+b-n, & \text{if not.} \end{cases}$$

Example 2.1.2

$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ under multiplication as LOC. Identity 1, inverse $\frac{1}{x}$. Inside $\mathbb{C}^*$ the unit circle $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ is also a group under multiplication. All of these are abelian.

Note:-

While it seems like the abelian pattern would continue as we construct higher dimensional sets comprised of $\mathbb{R}$, in fact, as we move to quaternions we run into our first non-abelian group constructed by $\mathbb{R}$ under multiplication.

Before we move onto more examples, some terminology updates are due:

Definition 2.1.5: Permutations of a set

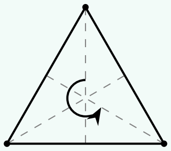
A permutation of a set A is a bijection $f : A \leftrightarrow A$, to form a group we use composition (functional or relational?) as our LOC and call this group Perm(A). Note that for Perm(A) its order, if finite, is given by $n!$ where n is the order of A.

Definition 2.1.6: Symmetric groups

A symmetric group on n elements is given by $S_n = \text{Perm}(\{1, \ldots, n\})$.

Example 2.1.3 (Symmetries of an equilateral triangle)

S_3 can be thought of as symmetries of a triangle comprised of rotations and reflections (3 of each, with one of the rotations being the identity).



Symmetires, then, permute the certices, and every permutation of the set of vertices arises from exacly one symmetry. Thus, S_3 occurs as the group of symmetries of a triangle. The other groups in $\mathbb{R}^2$ that arise from symmetries are called dihedral groups, and the groups comprised of symmetries in $\mathbb{R}^3$ are called octahedral groups. We will return to these at a later point.

Example 2.1.4 (Matrix groups)

We have some special type of matrix groups, it is okay if you do not know much about them at the moment, we will dive into detail about them later; note that the following groups are all using the LOC of matrix multiplication. The first such group is the ***general linear group*** given by $\text{GL}_n(\mathbb{R}) := \{\text{inverstible } n \times n \text{ matrices with real coefficients}\}$, the second is known as the ***special linear group*** given by $\text{SL}_n(\mathbb{R}) := \{n \times n \text{ real matrices with determinant } 1\}$, there also exists these for $\mathbb{C}$, and in fact for any $\mathbb{F}$ as we will later show from $\text{GL}(n, \mathbb{F})$ (you do not need to know what this means for now).

A group that has the property of being generated by an element (in example 2.0.3, the element that generates is a single symmetry) such that the entire group can be obtained by adding said element and/ or its inverse to itself repeatedly is said to be ***cyclic***.

2.2 Constructions

A natural question that arises in the course of group study asks, *how can we construct new groups from existing groups?* That is to say, how can one *combine* groups? We combine groups using *products* given by $G \times H$ such that G, H are both groups; the underlying set is given by ordinary Cartesian product, and the law of composition is said to be given termwise; i.e.,

$$(a, b) \cdot (a', b') \coloneqq (aa', bb').$$

There are times we may use the term *sum* for the combination of G and H, written $G \oplus H$, but we usually have more specific uses for this term (though this may not *always* be the case). For construction on more than two groups we simply have

$$G_1 \times \ldots G_n \coloneqq \{(a_1, \ldots, a_n) \mid a_i \in G_i\}$$

with LOC given by

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) \coloneqq (a_1 b_1, \ldots, a_n b_n).$$

When taking the product of n groups (i.e., G^n (e.g., $\mathbb{Z}^n$)) we usually denote this via

$$\bigoplus_{i=1}^{n} G_i \text{ or } \prod_{i=1}^{n} G_i.$$

When given infinitely many groups, our summation symbol takes on a special property, wherein $\prod_{i=1}^{\infty} G_i = \{(a_1, a_2, \ldots) \mid a_i \in G_i\}$, but $\bigoplus_{i=1}^{\infty} G_i = \{(a_1, \ldots) \mid a_i \in G_i,$ where all but finitely many a_i are identity$\}$. We can see this best exemplified with some polynomials:

Example 2.2.1 (Power series and polynomial groups)

Consider $G_0 = G_1 = \ldots = (\mathbb{R}, +)$ for $(a_0, a_1, \ldots)$ by $\sum_i^n a_i x^i$, then

$$\prod_{i=0}^{\infty} \mathbb{R} = \mathbb{R}[[x]], \text{ i.e., formal power series } \sum_{i=0}^{\infty} a_i x^i \text{ under addition,}$$

and

$$\bigoplus_{i=0}^{\infty} \mathbb{R} = \mathbb{R}[x], \text{ i.e., polynomials } \sum_{\text{finite}} a_i x^i.$$

2.3 Subgroups and Homomorphisms

Similar to how we have had subsets, we, too, have ***subgroups***!

Definition 2.3.1: Subgroups and proper subgroups

A ***subgroup*** H of G is a non-empty subset $H \subset G$ which is closed under the given law of composition—that is to say, $\forall a, b \in H \implies ab \in H$—and inversion—i.e., $\forall a \in H \implies a^{-1} \in H$. Since $H \neq \emptyset$, those 2 conditions imply $e \in H$. Thus H under the same operation as G is a group within its own right. We say that H is a ***proper subgroup*** if $H \subset G$ but $H \neq G$.

Theorem 2.3.1

Let S be a subgroup of $(\mathbb{Z}, +)$ (somtimes represented as $\mathbb{Z}^+$). Either $S = \{0\}$—the trivial subgroup—or it is the form $\mathbb{Z}a$ such that a is the smallest positive integer in S.

Proof: Refer to Artin Ch.2, Thm.2.3.3. □

Proposition 2.3.1 Title

Let $a, b \in \mathbb{Z}$, not both zero, and let d be their greatest common divisor, the positive integer that generates the subgroup $S = \mathbb{Z}a + \mathbb{Z}b$. So $\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b$. Then

(a) d divides a and b;

(b) if an integer n divides both a and b, it, too, divides d;

(c) there are integers r and s such that $d = ra + sb$.

Corollary 2.3.1

A pair $a, b \in \mathbb{Z}$ is relatively prime $\iff$ there are integers r and s such that $ra + sb = 1$.

Corollary 2.3.2

Let $p \in \mathbb{P}$. If p divides a product of $ab \in \mathbb{Z}$, then p divides a XOR p divides b.

Definition 2.3.2: Homomorphisms and isomorphisms

Given two groups G, H, a ***homomorphism*** (abbr. homom. or hom.) $\varphi : G \longrightarrow H$ is a map which respects the law of composition and is such that $\forall a, b \in G, \varphi(ab) = \varphi(a)\varphi(b)$. This implies $\varphi(e_G) = e_H$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$. An ***isomorphism*** (abbr. isom.) is a bijective homomorphism. If G and H are isomorphic, they are essentially the "same" group structure-wise, even if its elemnts and laws may have different names!

Lecture 3.

Group Relations

3.1 Symmetry Group

3.2 Group Relations

3.2.1 Subgroups

3.2.2 Homomorphisms

3.2.3 Kernals, Images, and Order

3.2.4 Finite Symmetric Groups

Lecture 4.

Quotient Groups

4.1 Cardinality

4.2 Sets of Maps and Powersets

4.3 Equivalence Relations

4.4 Quotient Groups

4.5 Congruence mod H