

MATH 30A NOTES 2009

CONTENTS

0. Introduction	2
0.1. Induction	2
0.2. Bijection (a)	2
0.3. Bijection (b)	3
0.4. Bijection (c)	4
0.5. Bijection (d)	4
0.6. Axiom of Choice	5
0.7. Power set	5
0.8. Relations and Cartesian products	6
0.9. Partitions and equivalence	7
0.10. Rhyme schemes and equivalence relations	8

0. INTRODUCTION

Algebra is the study of sets with binary operations. So, we will be talking about sets throughout the entire semester. I will spend the first two days reviewing set theory. Note that Math 23 is a prerequisite or corequisite for this course.

My main objective in this course is to teach students the language of Algebra: to understand the definitions and questions and be able to talk about it.

Review of set theory:

- a) Induction.
- b) Bijections and cardinality
- c) Power set
- d) Equivalence relations, congruence modulo n

0.1. **Induction.** Show by induction on n that

$$1 + 4 + 9 + 16 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

The basis for the induction is: When $n = 1$ this statement is true.

Now suppose by induction that $n \geq 1$ and the statement holds for n . Then we need to show that it holds for $n + 1$. On the LHS we have:

$$\begin{aligned} 1 + 4 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + \frac{(n+1)(6n+6)}{6} \\ &= \frac{(n+1)[2n^2 + n + 6n + 6]}{6} \end{aligned}$$

On the RHS we have:

$$\begin{aligned} \frac{(n+1)(n+2)(2(n+1)+1)}{6} &= \frac{(n+1)(n+2)(2n+3)}{6} \\ &= \frac{(n+1)[2n^2 + 7n + 6]}{6} \end{aligned}$$

So, $LHS = RHS$ and the equation holds for $n + 1$.

0.2. **Bijection (a).** Prove that a differentiable function $f : \mathbb{R} \rightarrow \mathbb{R}$ whose derivative is always positive is 1-1 but not necessarily onto.

I used this example to explain the basic properties of mappings. First of all a *function* or *mapping* has three parts: a set A called the *domain* of f , a set B called the *codomain* of f and the function f . We write:

$$f : A \rightarrow B$$

For every $a \in A$ we get one element $f(a) \in B$. In set theory, where everything is a set, the function f is identified with its graph

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

which is explained below.

Problem (a) has two parts. The first part is to prove that any differentiable function with positive derivative is 1-1. The second part is to find an example of a function with these properties which is not onto.

I reviewed the definitions. *Surjective* or *onto* means that $f(x)$ gives all values on the right hand side of the arrow $f : \mathbb{R} \rightarrow \mathbb{R}$. For example, $f(x) = x^2$ is not onto \mathbb{R} . The formal definition is:

Definition 0.1. $f : A \rightarrow B$ is surjective or onto if, for every $b \in B$ there exists an $a \in A$ so that $f(a) = b$.

Someone came up with the example

$$f(x) = e^x$$

This is not surjective since e^x is always positive.

Definition 0.2. A function $f : A \rightarrow B$ is defined to be 1-1 if it sends two elements to two elements ("2-2" would be a better way to say this). In other words, any two distinct elements $a, b \in A$, $a \neq b$ go to two distinct elements of B : $f(a) \neq f(b)$.

So, to prove f is 1-1 we take two distinct elements of the domain $x_1, x_2 \in \mathbb{R}$. One of them will be bigger than the other, say $x_2 > x_1$. Then by the fundamental theorem of calculus we have

$$f(x_2) = f(x_1) + \int_{x_1}^{x_2} f'(x) dx$$

Since $f'(x) > 0$ for all x , its integral is positive:

$$\int_{x_1}^{x_2} f'(x) dx > 0$$

Therefore, $f(x_2) > f(x_1)$. In particular $f(x_2) \neq f(x_1)$. So f is 1-1.

0.3. Bijection (b). If there is a mapping of sets $f : A \rightarrow B$ which is 1-1 but not onto then what can you say about the cardinality of the sets A, B ?

If f is not onto then B has at least one more element than A . This means that

$$|A| < |B| \text{ if } A \text{ is a finite set.}$$

The correct answer in general is:

$$|A| \leq |B|$$

Here $|A|$ denotes the *cardinality* of the set A . This is the number of elements of A . However, it can be various degrees of infinity. Cardinality will not play a large role in this course. So, I don't want to prove theorems about cardinality. I just want to discuss the concept and history.

If A, B are infinite sets then it could happen that they have the same number of elements and there might be a 1-1 mapping which is not onto. In fact, this is the definition of an infinite set.

Definition 0.3. *A set A is infinite if there exists a mapping $f : A \rightarrow A$ which is 1-1 but not onto.*

For example, the infinite set $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ has a 1-1 mapping $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ which is not onto given by $f(n) = 2n$.

0.4. **Bijection (c).** *Find a function $\mathbb{Z} \rightarrow \mathbb{Z}$ which is surjective but not 1-1.*

The first answer we got which I simplified here was:

$$f(n) = \begin{cases} n & \text{if } n < 2 \\ n - 1 & \text{if } n \geq 2 \end{cases}$$

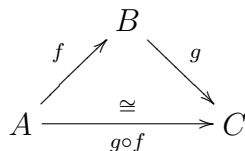
Since $f(1) = 1$ and $f(2) = 1$, this function is not 1-1. Then I asked for a formula with only one equation which would be easier to type and someone gave the example:

$$f(n) = \left\lceil \frac{n}{2} \right\rceil$$

where $\lceil - \rceil$ means *round up* to the nearest integer.

0.5. **Bijection (d).** *Suppose that $f : A \rightarrow B$ and $g : B \rightarrow C$ are mappings of sets so that $g \circ f : A \rightarrow C$ is a bijection. Then what can you say about f and g ?*

The answer is: f is an injection and g is a surjection. I asked for a proof that g is surjective. Here is a diagram which may be helpful.



Then we went through the proof that g is onto. First, recall the definition: g onto means that for every $c \in C$ there is a $b \in B$ so that $g(b) = c$. This is what we want to prove. We know that $g \circ f : A \rightarrow C$ is a bijection. Then implies that for every $c \in C$ there is a $a \in A$ so

that $(g \circ f)(a) = c$. But then $b = f(a)$ is an element of B which maps to c :

$$g(b) = (g \circ f)(a) = c.$$

So, g is surjective.

0.6. Axiom of Choice. The definition of g being *onto* suggests that we have a function from C to B . Call this s . Then for each $c \in C$ we have $b = s(c)$ so that $g(s(c)) = g(b) = c$. This means that $g \circ s : C \rightarrow C$ is the *identity mapping*: $g \circ s = id_C$. The existence of such a function s is called the *Axiom of Choice*.

$g : B \rightarrow C$ being surjective means that for each element $c \in C$ separately we can find $b = s(c)$. The Axiom of Choice says that we can do it all at once (make an infinite number of random choice at one time).

0.7. Power set. If A is any set, the *power set* $\mathcal{P}(A)$ is the set of all subsets of A . The cardinality of the power set is

$$|\mathcal{P}(A)| = 2^{|A|}$$

For example, if $A = \{a, b, c\}$ then $\mathcal{P}(A)$ has $2^3 = 8$ elements and they are:

$$\begin{aligned} & \{ \} \\ & \{a\}, \quad \{b\}, \quad \{c\} \\ & \{a, b\}, \quad \{a, c\}, \quad \{b, c\} \\ & \{a, b, c\} \end{aligned}$$

These sets can be written in a binary code as follows:

$$\begin{aligned} & 000 \\ & 100, \quad 010, \quad 001 \\ & 110, \quad 101, \quad 011 \\ & 111 \end{aligned}$$

The famous Cantor diagonalization argument shows the following theorem. You don't need to know the proof of this statement.

Theorem 0.4 (Cantor). *For any set A , the cardinality of $\mathcal{P}(A)$ is always strictly greater than the cardinality of A :*

$$|\mathcal{P}(A)| > |A|.$$

We checked that this is true in the case when $A = \{ \} = \emptyset$ is the empty set. Then $|A| = 0$, but $\mathcal{P}(A)$ has one element, namely, the empty set is a subset of the empty set:

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

and

$$|\mathcal{P}(A)| = 2^0 = 1$$

as the formula says.

0.8. Relations and Cartesian products. The *Cartesian product* $A \times B$ of two sets A, B is the set of all ordered pairs (a, b) where $a \in A, b \in B$. This is useful since the *graph* of a function $f : A \rightarrow B$ is a subset of the Cartesian product:

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

A *relation* \mathcal{R} on a set A is defined to be any subset of the Cartesian product $A \times A$. If $(a, b) \in \mathcal{R}$ then we write $a\mathcal{R}b$. For example, the relation $\mathcal{R} = (\leq)$ on \mathbb{R} is the set of all pairs of real numbers (x, y) so that $x \leq y$:

$$(\leq) = \{(x, y) \mid x, y \in \mathbb{R}, x \leq y\}$$

I put parentheses around the relation since $\mathcal{R} = \leq$ looks stupid.

If you shade in this set you note

- (1) The set includes the diagonal $\Delta = \{(x, x) \mid x \in \mathbb{R}\}$
- (2) The set is only above the diagonal and not below. So, it is not symmetric around the diagonal.

Definition 0.5. A relation \mathcal{R} on a set A is called

- (1) reflexive if $x\mathcal{R}x$ for all $x \in A$
- (2) symmetric if $x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- (3) transitive if $x\mathcal{R}y, y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

The relation \leq is reflexive and transitive but not symmetric.

Draw a picture of a symmetric relation on the set of real numbers.

Explain why the drawing fits the definition.

Here is a problem which combines these concepts.

Show that $2^n > n^2$ for all integers $n \geq 5$. Give an interpretation in terms of sets. Does this make sense when n is infinite?

The proof is in the homework 1 instructions. The interpretation is:

If A is a set having at least 5 elements then the power set of A has strictly greater cardinality than the Cartesian product $A \times A$.

0.9. Partitions and equivalence.

Definition 0.6. A partition of a set A is a covering of A by disjoint nonempty subsets:

$$A = \coprod A_i$$

This means two things:

- (1) The subsets A_i cover A in the sense that every element of A is in one of the subsets A_i . In symbols this is:

$$A = \bigcup A_i$$

In other words, A is the union of the sets A_i .

- (2) The subsets A_i are disjoint. They don't overlap. In symbols: $A_i \cap A_j = \emptyset$ if $i \neq j$.

The symbol \coprod means disjoint union.

Often sets are partitioned. For example, real numbers are often partitioned into positive, negative and zero:

$$\mathbb{R} = \mathbb{R}^+ \coprod \mathbb{R}^- \coprod \{0\}$$

Partitions have the property that every element of the set lies in exactly one "part" or "cell" and no cell is allowed to be empty.

One extremely important example that we will use is the partition of the set of integers according to their remainder after dividing by some number n . For example, if $n = 10$ then we can partition the set \mathbb{Z}^+ of positive integers into ten cells according to their last digit. All positive integers ending in 1 are in one cell, etc. So, the cells of this partition are:

$$\begin{aligned} A_1 &= \{1, 11, 21, 31, \dots\} \\ A_2 &= \{2, 12, 22, 32, \dots\} \\ A_3 &= \{3, 13, 23, 33, \dots\} \\ A_4 &= \{4, 14, 24, 34, \dots\} \\ &\vdots \\ A_0 &= \{10, 20, 30, 40, \dots\} \end{aligned}$$

The last set A_0 is the set of all positive multiples of 10:

$$A_0 = \{10n \mid n \in \mathbb{Z}^+\}$$

For $k > 0$ the formula is:

$$A_k = \{10m + k \mid k \in \mathbb{Z}^{\geq 0}\}$$

Given a partition of a set A , we have a relation on this set which is "being in the same cell" So, two elements of A are related if they are

“cell-mates.”

$$x \sim y \Leftrightarrow x \text{ and } y \text{ are in the same cell}$$

I gave the example of a prison since the words and pictures suggest this. If x is your cell-mate and y is a cell-mate of x then y is also your cell-mate because you are all in the same cell! So, being cell-mates is transitive. You can think about why it is reflexive and symmetric.

Another example is $x \sim y$ if x, y are positive integers which have the same last digit in base 10. The last digit is equal to the remainder when dividing by 10. We could take other bases and say $x \equiv_n y$ if x, y have the same remainder when divided by n . For example $x \equiv_2 y$ means that x, y have the same *parity* which means they are either both even or both odd.

0.10. Rhyme schemes and equivalence relations. Around 1950, H.W. Becker wrote a series of papers giving a classification of all possible rhyming schemes and counting the number of rhyming schemes of each kind. What does this have to do with partitions and equivalence relations?

I showed an example using the second stanza of John Keats “Ode to a nightingale”. This has 10 lines with last words and rhyming scheme given in the following chart.

Line	last word	rhyme scheme
1	been	a
2	earth,	b
3	green,	a
4	mirth!	b
5	South,	c
6	Hippocrene,	a
7	brim,	d
8	mouth;	c
9	unseen,	a
10	dim:	d

The rhyming scheme is *abab cad cad*. This gives a partition of the set of lines:

$$a = \{1, 3, 6, 9\}$$

$$b = \{2, 4\}$$

$$c = \{5, 8\}$$

$$d = \{7, 10\}$$

The set of lines (actually line numbers) is $A = \{1, 2, \dots, 10\}$. Lines 1,3,6,9 rhyme so we put those lines into one set. (But we use only the numbers of the lines.) We have a relation on the set A , namely,

$$j \sim k$$

if Line j rhymes with Line k . This is

- (1) reflexive: Each line rhymes with itself.
- (2) symmetric: E.g.: since Line 2 rhymes with Line 4, it is also true that Line 4 rhymes with Line 2.
- (3) transitive: E.g.: Line 1 rhymes with Line 3 and Line 3 rhymes with Line 9 and therefore Line 1 rhymes with Line 9.

Therefore, “rhyming” is an equivalence relation.

Definition 0.7. *An equivalence relation of a set A is any relation which is reflexive, symmetric and transitive.*

What does this mean geometrically on the graph? Here is an example giving a typical graph:

$$\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \lfloor x \rfloor = \lfloor y \rfloor\}$$

where $\lfloor x \rfloor$ is the greatest integer $\leq x$, i.e., it is the integer part of x . The equivalence relation \mathcal{R} is “having the same integer part”

Theorem 0.8. *A partition of a set gives an equivalence relation of being cell-mates and an equivalence relation on a set A gives a partition of the set into equivalence classes:*

$$[a] = \{x \in A \mid x\mathcal{R}a\}$$

The proof is on page 8 of the book. We will discuss the theory of equivalence relations again when we get to factor groups.