Math 113, Fall 2019
Lecture 1, Thursday, 8/29/2019

CLASS ANNOUNCEMENTS:

Homework due Sept 5, in-class:
§0 : 9, 12, 16, 17, 26, 32, 34
§1 : 3, 8, 22, 25, 30, 32, 26
Readings for Tuesday: §0, 1, 2
iClickers required for the course, starting Tuesday.

Topics Today:

- Introduction
- Basics of Sets
- Functions
- Cardinalities
- Relations (if time permits)

1 Syllabus

Instructor: Paul Vojta (vojta@math.berkeley.edu)
(pronounced 'Voyta')

Lectures: T/Th 12:30-2pm, Etcheverry 3107
(https://math.berkeley.edu/ vojta/113.html)

OH: T/TH 10:30am - 12pm

Course Description: Sets and relations. The integers, congruences, and the Fundamental Theorem of Arithmetic. Groups and their factor groups. Commutative rings, ideals, and quotient fields. The theory of polynomials: Euclidean algorithm and unique factorizations. The Fundamental Theorem of Algebra. Fields and field extensions.

Textbook Sections: 0-11, 13-16, 18-23, 26, 27, 29-31, 45-47, 32, 34.

Homeworks: Due weekly on Thursdays, physical copy in class.
Comment: "I tend to follow the book rather closely, but try to give interesting exercises and examples."

2 Grading

20%	Homework	Assigned weekly	Due in class, usually on Thursdays
20%	First midterm	TBD	12:30–2:00 pm
25%	Second midterm	TBD	12:30–2:00 pm
35%	Final exam	Friday, December 20	8:00–11:00 am

3 Quoting Results: Homeworks

General rules on homework assignments are:

- For any assigned problem from the book, you may use without proof any earlier exercise in the book.
- For an assigned problem not from the book, you may use without proof any exercise in the book that occurs in or before the section containing the most recent problem from the book in the assignment prior to the problem.
- When doing a problem from a given section of the book, you may not use material from subsequent sections of the book (even if problems from those sections are also in the homework assignment). (For problems not from the book, use the principle in the previous bullet point.)

4 Brief Overview of the Course:

We'll be talking about Groups, Rings, Fields abstractly. We should already know the sets

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

and notice that we define:

$$\mathbb{N} := \{0, 1, \dots\},$$

as opposed to in Math 104.
Further, in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, if we only look at $+$ and $-$ (ignore $\times, /$, inequalities, limits, $\frac{d}{dx}$, $\int$) then these are **examples of groups**.

4.1 Other Examples of Groups

- $n \times m$ matrices, equipped with $+$ or $-$.
- Vector Spaces (ignoring scalar multiplication)
- $n \times n$ **invertible** matrices with matrix multiplication.
  - We say that AB^{-1} takes the role of subtraction in this group (non-commutative).
- nonzero real numbers under $\times, /$

4.2 Examples of Rings

The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $+, -, \times$ are examples of **rings**. Other examples include $n \times n$ matrices. The sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $+, -, \times, /$ are examples of **fields**. We can think of polynomials as rings too.

5 A Word About Abstraction:

In Math 54, we definied an **abstract vector space**, assumed to have the operation of .
To study the solutions of a rubrics cube, we can use group theory. Alternatively, the 15-puzzle of 4×4 locations and one missing square, where we slide around tiles to get a particular pattern.

Vojta gives the example that if we start with

$$\begin{bmatrix} 15 & 14 & 13 & 12 \\ 11 & 10 & 9 & 8 \\ 7 & 6 & 5 & 4 \\ 3 & 1 & 2 & \times \end{bmatrix}$$

(with exactly two with order swapped), then it turns out we **cannot** get this to pure descending order as below

$$\begin{bmatrix} 15 & 14 & 13 & 12 \\ 11 & 10 & 9 & 8 \\ 7 & 6 & 5 & 4 \\ 3 & 2 & 1 & \times \end{bmatrix}$$

We'll see why this is the case via Group Theory.

6 Introductory Material

We should already know the sets:

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

and the symbols:

$$\forall, \exists, \cup, \cap, \in, \notin, \subseteq, \subset, \supset, \supseteq$$

Vojta notes that he uses $\subsetneq$ and $\supsetneq$ for $\subset, \supset$, respectively.
We also have that

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

where A_i are all sets. Similarly for intersections $\cap$.
Also,

$$\bigcup_{i \in I} A_i = \{x | x \in A_i \text{ for some } i\} = \{x | \exists_{i \in I} : x \in A_i\}$$

where I and A_i are sets $\forall_{i \in I}$, we may take a union over an **indexing set** I.
So,

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i \in \{1, \ldots, n\}} A_i,$$

where n can be ∞.

6.1 What if $I = \{\}$?

Looking at our above definition $\{x | \exists_{i \in I} : x \in A_i\}$, we see this condition can never be satisfied.
However, consider:

$$\bigcap_{i \in I} = \{x : x \in A_i \forall_{i \in I}\}$$

and notice this works for $I := \{\}$. This is problematic (as can be seen from a logic course), so we use that if $A_i \subseteq X \forall_i$, then

$$\bigcap_{i \in I} A_i = X \setminus \cup_{i \in I} (X \setminus A_i) \text{ if } I \neq \{\}$$

If $I = \{\}$, the answer depends on X. Usually we can tell from the context what X is.

Break time.

Vojta enters break-time, distributing a handout on sets, relations, and partitions (although we likely won't get to partitions today).

Definition: Well Defined -

- Uniquely defined (independent of any choices made)
- Is the sort of object that it is claimed to be

For example of violating the first, an empty intersection is **not** uniquely defined because it depends on the choice of X. We can make this uniquely defined by specifying X.
A qualifying example is the dimension of a vector space, where we prove that every vector space has at least one basis, and show that the dimension is unique regardless the choice of basis.

Definition: Cartesian Product -

The Cartesian product of sets A and B is:

$$A \times B := \{(a, b) : a \in A \text{ and } b \in B\},$$

and we can also write this as:

$$\prod_{i=1}^{n} A_i \text{ or } \underbrace{\prod_{i \in I} A_i}\text{,}$$

where this is a set of 'set of choice functions' $\phi : I \to \cup A_i$ such that $\phi(i) \in A_i \forall_i$. Note that these are ordered pairs.

Definition: Functions -

Let A, B be sets. A **function** $f : A \to B$ is a subset $\Gamma \subseteq A \times B$ with the following property:

$$\forall_{a \in A}, \exists!_{b \in B} : (a, b) \in \Gamma$$

which is essentially the vertical line test. This element is denoted as $f(a)$. Here, A is called the **domain** of f, and B is called the **codomain** of f.

We say that Γ is the **graph** of f, and $f[A] := \{f(a) : a \in A\}$ is called the **range** of f.

Example:

$$f = \{(x, \sin x) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$$
$$x \overset{f}{\mapsto} \sin x$$

is a function from $\mathbb{R}$ to $\mathbb{R}$. We write this as $f : \mathbb{R} \to \mathbb{R}$.
In this example, we say that Γ is the graph of f with range $= [-1, 1]$ (the interval).
We should also know **injective, surjective, bijective** functions.

Definition: Injective -

A one-to-one function is an injective function, and we also call this an injection. This is such that

$$f(x) \neq f(y), \forall_{x \neq y}$$

in the domain.

Definition: Surjective -

An onto function is a surjective function, and we also call this a surjection. This is such that

$$\text{range of } f = \text{codomain}$$

Definition: Bijective -

A function that is both injective and surjective is said to be **bijective**.

Definition: Inverse Functions -

If $f : A \to B$ is a bijective function, then it has an **inverse function**

$$g = f^{-1} : B \to A,$$

characterized by $f(a) = b \iff g(b) = a, \forall_{a \in A, b \in B}$, or by $f \circ g = \mathrm{id}_B$ which is the identity function $b \mapsto f(g(b))$, and $g \circ f = \mathrm{id}_A$.

7 Cardinalities:

Definition: Cardinality -

Sets A and B have the same **cardinality** if and only if there is a **bijection** from $A \to B$.

Remark: Vojta notes that in definitions, we'll usually simply state 'if' to mean 'if and only if'. However, in these notes I will make an effort for clarity sake to explicitly write 'if and only if' in this case.

Example: One can show: Let $m, n \in \mathbb{N}$. Then the sets $\{1, 2, \ldots, m\}$ and $\{1, 2, \ldots, n\}$ have the same cardinality if and only if $m = n$. (For our purposes, we define that if $m, n = 0$, then this is the empty set.)

We can make the following definition:

Definition: Finite -

A set is **finite** if it has the same cardinality as $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. If so, then we say that the set is **finite**, and that the number of elements is n. (This is well-defined and agrees with common usage).

Continuing with this definition, if a set is not finite, then it is **infinite**.

Remark: Here $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all **infinite**. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ all have the same cardinality, and $\mathbb{N}, \mathbb{R}$ **do not** have the same cardinality (proved in 55 or 104).

The following definition is **different from what is given in the book**:

Definition: Relation $\mathcal{R}$ -

A **relation** on a set S is a subset $\mathcal{R}$ of $S \times S$.

Lecture ends here.