Notes for 1st Jan (Tuesday)

1 Logistics

Please check the webpage (`http://www.math.iisc.ac.in/~vamsipingali/um2032018.html`) **regularly**. Check it like your life depends on it. The homeworks, exam dates, and everything else will be on the darned webpage!

There are two teaching assistants for this course - K. Hariram, and Abhash Kumar Jha. If you have questions/doubts, first ask them, and then come me (after emailing me that is). If your roll number is odd, you are assigned to Hariram and if not, to Jha.

The grading policy is as follows :

1. Tests based on HW - 15 %. There will be a homework given fortnightly. There will be a test conducted by your TA (on the days of the tutorial session) consisting of 1 or 2 problems which are drawn from the assigned HW problems for that week.

2. Midterm - 35 %. The syllabus for the Midterm is everything we will have done till then.

3. Final - 50% : The date and place will be announced later. The syllabus is everything we will have covered in this course.

2 Textbooks

1. Algebra part mostly from "A concrete introduction to higher algebra" by Lindsay N. Childs (Third Edition).

2. Number theory from Childs and "Concrete Mathematics" by Donald Knuth.

3. Some group theory possibly from "Groups and symmetry" by M. A. Armstrong.

4. Combinatorics and graph theory from "A walk through combinatorics" by Miklos Bona.

5. A fun read is "Elements of Algebra" by John Stillwell.

3 Trailer

At the end of this class I hope to teach you enough so as to appreciate the following.

1. Is the formula like the quadratic formula for higher degree polynomials ? Why is it unreasonable to expect such a formula for degree ≥ 5 ? (Field theory)

2. Devise a walk through the city of Könisberg that crosses each of its bridges exactly once. (Graph theory)

3. Find an integer x such that it leaves a remainder a_1 when divided by n_1, a_2 when divided by n_2 and so on. (Number theory + Ring theory)

4. Can you express $x_1^3 + x_2^3 + \ldots + x_{100}^3$ in terms of $x_1 + x_2 \ldots + x_{100}, \sum x_i x_j, \sum x_i x_j x_k$, etc ? (Polynomials)

5. How does one secure information on the internet ? (Cryptography through group theory)

and more.....

4 What is at the bottom of mathematics ?

Mathematics is a human construct. Clearly, one needs some "real world" element to even start talking about mathematics (either a human or a computer plugged into a socket). What lies at the interface of the real world and mathematics ? In other words, where must we begin ?

One might think that set theory is at the bottom of mathematics. After all, in high school we were plagued with nonsense like Venn Diagrams and so on. All that better have a point! Speaking of high school,, back then, everything was a set. The phrase "Set of all sets" wouldn't have raised eyebrows. But the philosopher Bertrand Russell came up with the following famous paradox (the "barber paradox") -

If there is only one barber in London who shaves all those and only those who do not shave themselves, then who shaves the barber? (In India the question is easy - Not everyone needs to be shaved! But we are talking of prissy London here.) If the barber shaves himself, he violates his constraint. If he does not shave himself, then by definition he has to shave himself!

More formally, consider the set A defined as the set of all sets that do not contain themselves as elements. This set cannot exist! The point is that not everything defined by an English sentence should be considered as a set. In other words, we need to have axioms that tells how to construct sets from "standard", "God-given" sets.

You might (rightly) have the following objection. If you want to axiomatize set theory itself, then you have to use phrases like "for all sets that something blah, there exists blah". But "for all" and "there exists" are themselves part of logic. But should we axiomatise logic itself ? If so, in terms of what ? (Normally when you do a course on logic, they use words like "functions" and "sets".) Don't we have a danger of circularity ? We do but can we mark clearly the interface between the real world and mathematics ?

The way out is the following. We (humans or computers) are assumed to be able to write "finite" strings from a "finite" alphabet consisting of the following symbols :

$\forall$, $\exists$, $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$, parantheses, comma, the constant ϕ (empty set), the binary predicates/relationships $=$ and $\in$, and an infinite collection of variables $x_1, x_2, \ldots$ (You can instead use $|, ||, |||\ldots$ if you are uncomfortable with using numbers $1, 2, \ldots$)
whilst "following" some "rules" (the capabilies assumed are pattern matching, substitution into formulas, and recursion). Notice that already we are assuming that we understand what the terms in quotes mean. So we are already assuming a little bit of natural numbers as "God-given" (as Kronecker would have said).

There are two kinds of strings we can write - Terms (i.e. just writing variables and constants) and formulas (things that have a truth value). There are some rules of deduction (like $P \Rightarrow Q$) that allow us to come up with new formulas from old ones. We need some formulae to begin with in order to find new ones. These formulae are the "axioms" of set theory. Now one can write every mathematical theorem as a formula in this language. (Read Yuri Mannin's book or ask Siddhartha Gadgil for further details.)

In other words, the capabilities of a computer language like C++ is enough to do mathematics. You can write all the axioms of set theory (and logic itself) in C++. When you run the program, you connect the abstraction to real life.

Rather than going in this formal route, we will follow Terence Tao (and Paul Halmos's book "Naive set theory") and simply write the axioms of set theory in simple English with the understanding that we know "intuitive logic". The axioms in Tao's book are somewhat redundant but convenient nonetheless. The axioms are called "Zermelo-Fraenkel" axioms (ZF). There is a controversial axiom called axiom of choice that every self-respecting mathematician believes. So the axioms will be ZFC (Zermelo-Fraenkel with choice).

5 Naive set theory done right - ZFC

"Definition" of a set - A set A is any "unordered collection" of objects. A "subset" A of B is a set all of whose elements are elements of B. Of course, all of this is too vague and dangerous. Basically, we will not define sets. Rather we will say that whatever sets are, they follow the following axioms and you can construct new sets from old ones in the such and such ways. (So already, the phrase "Set of all sets" should raise eyebrows.) Here are the "axioms" from Terence Tao's book on real analysis :

1. If A is a set, then A is a valid object. In particular, given another set B you are allowed to ask whether A is an *element* of B. In fact, unlike Terence Tao (and like Paul Halmos) as far as we are concerned, *every* object is a set. (For example, the number 0 will be considered to be the empty set ϕ, the number one as the set containing the empty set $\{\phi\}$ and so on.)

2. Equality : Two sets are equal if and only if they contain the same elements (objects will be called elements from now onwards). (So order does not matter.)

3. Empty set : So far, we have no sets yet. So we postulate that there exists a set ϕ that does not contain any elements. (Of course by the previous axiom this set is unique.)

By the way, this means (by trivial logic) that every non-empty set has some element x, i.e., we can "choose" an element from a non-empty set. In fact, we can prove that one can "choose" elements from *finitely* many non-empty sets (we need induction to do this). But can we "choose" elements from each set of a family of infinitely many non-empty sets ? That is the axiom of choice that we will discuss later on.

4. Pairing : If A and B are sets, there exists a set containing only A and B as elements.

5. Union : For any set (of sets because every object for us is a set anyway) $\mathcal{F}$ there exists a set containing every element of some set in $\mathcal{F}$. (The union of an arbitrary number of sets exists.)

6. Regularity : Every non-empty set X contains an element y such that X and y are disjoint.

7. Specification : Ideally, we would like to construct a set by saying "X is a set consisting of things that satisfy some property". This axiom makes this "set builder" way of doing things precise.
   If A is a set, and $P(x)$ is a "property" that may be true or false for an element x in A, then there exists a subset X of A consisting of $x \in A$ such that $P(x)$ is true. Note that this means that we can only construct *subsets* of already existing sets this way. So no Russell paradox can occur.
   By the way, this axiom allows us to define the intersection of two sets and complement of a set. So we can do our usual De Morgan laws and everything we learnt in high school using Venn diagrams. (They are all *theorems* that can be proven using these axioms.)

8. Replacement : So far we cannot take a set and "transform" it into a new set using a "definable function". This axiom takes care of that.
   Suppose A is a set, and for any element $x \in A$ and an object (i.e. set) y there is a statement $P(x, y)$ such that for each $x \in A$, there is at most one y for which $P(x, y)$ is true. Then there exists a set B consisting of all y such that $P(x, y)$ is true. We abbreviate such y as $f(x)$.

9. Infinity ("To see a world in a grain of sand and heaven in a wild flower; To hold infinity in the palm of a hand and eternity in an hour" - Blake) : So far, we have the empty set ϕ, using pairing we can construct a set containing the empty set $\{\phi\}$, using it again, $\{\phi, \{\phi\}\}$, and so on. But these are only "finite" sets. We need a set containing all of these sets. (It will be a set containing the natural numbers, secretly speaking.)
   There exists a set S containing the empty set as an element, such that if $y \in S$, then $y \cup \{y\}$ is also a member of S. This clearly contains all natural numbers but how does one "extract" the set of natural numbers from this ? For that we need axioms of natural numbers. These axioms will be described later. (Peano's axioms.)

10. Power set : Given a set X, there exists a set $P(X)$ containing exactly all the subsets of X.

You can construct cartesian products of sets using the above axioms. Thus we can talk of relations and functions between sets.