Notes for 2nd Jan (Wednesday)

1 The road so far...

1. Discussed logistics, textbooks, etc. Some ramblings about the foundations of mathematics.
2. Discussed the Zermelo-Frankel Axioms of Set theory. Out of these the important points you have to take home are that sets can be constructed only from pre-existing ones (like the empty set) and the concepts of Cartesian product of two sets, relations, and functions. We assume that everyone knows what injective, surjective, and bijective mean.

2 Naive set theory done right - ZFC

Axiom of choice : Let $\mathcal{F}$ be a set (of sets as always) containing an arbitrary number of elements each of which is a non-empty set. Let $U = \cup_i X_i$ be the union of all elements X_i of $\mathcal{F}$. Then there exists a "choice" function $f : \mathcal{F} \to U$ such that $f(i)$ is an element of X_i.

We shall not bother constructing the set of natural numbers $\mathbb{N} \subset S$. We shall assume that one can freely add, subtract, multiply, and exponentiate natural numbers.

3 Equivalence relations and partitions

In this course, a relation R between sets A and B is a subset of $P(A \times B)$. A special and useful kind of a relation (generalising the property of equality) is that of an equivalence relation -

An equivalence relation R between A and itself (unfortunately, sometimes a relation between A and itself is said to be "a relation on A") such that

1. Every element of A is related to itself, i.e., $(a, a) \in R \ \forall \ a \in A$. (This is called the property of reflexivity.)
2. If a is related to b then b is related to a, i.e., if $(a, b) \in R$, then $(b, a) \in R$. (Symmetry.)
3. If a is related to b, and b to c, then a is related to c, i.e., if $(a, b) \in R$, $(b, c) \in R$, then $(a, c) \in R$. (Transitivity.)

Here are examples and counterexamples :

1. Similarity is an equivalence relation on the set of all triangles. (Why is the set of all triangles a well-defined concept by the way ?)

2. The parity of numbers being the same is an equivalence relation.

3. Suppose $S = \{1, 2, 3, 4\}$. Then the relation "1 is related to all the numbers and they are all related to 1" is not an equivalence relation. Indeed, the relation is $(1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (3, 1), (4, 1)$. So it is not reflexive and transitive but it is symmetric. Even if we include $(2, 2), (3, 3), (4, 4)$ it will fail to be transitive. (Indeed, 2 is related to 1, 1 is related to 3 but $(2, 3) \notin R$.)

4. Suppose $S = \{1, 2, 3, 4\}$. The relation "Every number is only related to itself" is an equivalence relation (it is simply the equality relation).

5. Suppose $S = \{1, 2, 3, 4\}$. Then "1 and 2 are related to each other and themselves. Likewise for 3 and 4" is an equivalence relation.

6. In S above, "1 and 2 are related to each other and themselves. 3 is related only to itself. But 4 is related to itself and 2" is not an equivalence relation.

Note that in the above examples, an equivalence relation behaves like an equality in the sense that one group all the elements that are equivalent into bunches. To make this precise, we define the notion of a set partition -

A set partition of a set S is a collection of subsets $A_i \in P(S)$ such that $U_i A_i = S$ and all the A_i are pairwise disjoint.

Here is a very useful theorem that tells us how equivalence relations are constructed. Going further, we shall denote "a is related to b" by $a \sim b$.

Theorem 1. *An equivalence relation between S and itself partitions S (the partitions are called equivalence classes). Conversely, every partition of S arises from an equivalence relation.*

Proof. Define the equivalence class $[a]$ of an element $a \in S$ as the subset $\{x \in S | x \sim a\}$. Clearly every element is in some equivalence class. Suppose $x \in [a]$ and $x \in [b]$, then $x \sim a$, $x \sim b$. Hence, $a \sim b$. This means that $[a] = [b]$ if $[a] \cap [b] \neq \phi$. Therefore the set of equivalence classes partitions S.

Conversely, given a partition S_i of S, define the relation $x \sim y$ if they both belong to the same S_i, i.e., $(x, y) \in R$ if $x, y \in S_i$ for some i. This can be easily checked to be an equivalence relation and indeed the equivalence classes are the S_i. □

Note that the above theorem tells us how many equivalence relations there can be on any set. For instance, on the set $\{1, 2, 3\}$, there are 5 equivalence relations.

Here is a nice application of these things :

Lemma 3.1. *Define an involution $i : S \to S$ to be any function such that $i^2(x) = x \ \forall \ x \in S$. If S is a finite set with an odd number of elements, then i has an odd number of fixed points. Conversely, if i has an odd number of fixed points, then S is odd.*

Proof. Define a relation $x \sim y$ if $x = i(y)$ or if $x = y$. Then this relation is reflexive, symmetric $i(x) = i^2(y) = y$, and transitive $i(x) = y, i(y) = z \Rightarrow i(z) = i^2(x) = x$. Unless one has a fixed point, every equivalence class has exactly 2 elements. Therefore $2k + number of fixed points = |S|$. This observation completes the proof. □

Here is a spectacular (but completely uninformative) proof due to Don Zagier (based on ideas of Heath-Brown) that every prime number p of the form $4k + 1$ is the sum of two squares.

Proof. Let $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$. If $|S|$ is odd, then the involution $(x, y, z) \rightarrow (x, z, y)$ has a fixed points (and hence we are done). To prove that $|S|$ is odd, it is enough to show that the following map is an involution.

$$
\begin{aligned}
(x, y, z) &\rightarrow (x + 2z, z, y - x - z) \; if \; x < y - z, \\
(x, y, z) &\rightarrow (2y - x, y, x - y + z) \; if \; y - z < x < 2y, \\
(x, y, z) &\rightarrow (x - 2y, x - y + z, y) \; if \; 2y < x.
\end{aligned}
$$

This will be given as a HW. □

Before we end our discussion of equivalence relations, there is a very useful definition that occurs in many walks of algebra and topology : That of a quotient. The set of equivalence classes of an equivalence relation is called a quotient set. Here are examples.

1. The quotient set of the equivalence relation on $\mathbb{N}$ given by $x \sim y$ if x and y have the same parity is $\{[0], [1]\}$.

2. For the equivalence relation on $0 \leq x \leq 1$ given by $x \sim x \; \forall \; x$ and $0 \sim 1$, the quotient is bijective to $x^2 + y^2 = 1$ in $\mathbb{R}^2$.