Notes for 15th Jan (Tuesday)

1 The road so far...

1. Motivated graphs as data structures.
2. Defined permutations, combinations, and multisets. Illustrated the sum and quotient principles.

2 Pigeon hole, permutations and combinations

1. The number of k-element multisets from $[n]$ is $C(n+k-1,k)$. Another way is to define an equivalence relation among bookcase arrangements of distinct books saying we get the same arrangement by permuting the books. The number of arrangements is gotten by placing the first book (n ways), the second book $(n+1)$ ways (because it can be on either side of the first book), etc. Now the quotient principle gives the answer.
2. A city has ten recently built junctions. Some of these get traffic lights and some of those that get lights get a petrol pump. In how many different ways can this happen ?
   There is a bijection from this problem to that of 10-digit words over A, B, C (which is basically 3^{10} by the product principle). If the ith junction gets both a petrol pump and a traffic signal then put an A, if only a traffic light then B, and otherwise C.

3 Cycles in permutations

Since a permutation is simply a bijection of $[n]$, it makes sense to have more structure on S_n by defining a "multiplication" operation as composition of functions, i.e., $f.g = f \circ g$. (Unfortunately Bona uses another convention. According to that author, $f.g = g \circ f$.) For instance,

1. On $[3]$, suppose $f = 213$ and $g = 321$, then $f.g(1) = f(g(1)) = f(3) = 3$, $f.g(2) = f(2) = 1$ and $f.g(3) = f(1) = 2$. On the other hand, $g.f(1) = g(2) = 2 \neq f.g(1)$. So multiplicative is not commutative.
2. Likewise, on $[4]$, suppose $f = 1243$ and $g = f$, then $f.g = f^2(1) = f(1) = 1$, $f.g(2) = f(2) = 2$, $f.g(3) = f(4) = 3$ and $f.g(4) = 4$, therefore, $f^2 = id$.

In fact, it is not hard to see that for every permutation, there is a multiplicative inverse. Moreover, since function composition is associative so is multiplication of permutations. It is useful to study and count permutations using this structure. Turns out it this structure plays an important role in the rest of mathematics. It is an example of a group.

A group G is a set equipped with a binary operation $* : G \times G \to G$ satsifying

1. Associativity : $(a * b) * c = a * (b * c)$
2. Identity : There exists an element e such that $a * e = e * a = a \ \forall \ a \in G$.
3. Multiplicative inverse : Given any element a there exists a b (corresponding to a) such that $a * b = b * a = e$.

(BTW, a set with a binary operation satisfying the first two axioms is called a Monoid.) It is easy to prove that the identity and inverses are unique. S_n equipped with this multiplication operation is called the symmetric group on n letters. Other examples of groups are $(\mathbb{Z}, +), (Invertible\ n \times n\ matrices\ with\ real\ entries matrix\ multiplication)$. Groups where commutativity holds are called Abelian groups.

Here is an interesting lemma that generalises the phenomenon of the second example.

Lemma 3.1. *Let $p : [n] \to [n]$ be a permutation and let $x \in [n]$. Then there exists a positive integer $1 \leq i_x \leq n$ such that $p^{i_x}(x) = x$.*

Proof. There are n possible values for each of $p(x), p^2(x), \ldots, p^n(x)$. If none of these equals x, then by PHP $p^j(x) = p^k(x)$ for some $j < k$. Applying p^{-1} on both sides j times we see that $x = p^{k-j}(x)$ which is a contradiction. □

Now we make a definition : Let $p \in S_n$ and $x \in [n]$. Let i_x be the smallest integer such that $p^{i_x}(x) = x$. Then we say that $x, p(x), \ldots, p^{i_x - 1}(x)$ forms an i-cycle in p.

Lemma 3.2. *All permutations can be decomposed into the disjoint unions of their cycles.*

The proof will be given as a HW problem. Here are examples :

1. $p \in S_5$ given by $p = 321564$ can be written as (31)(2)(564).
2. $p \in S_4$ given by $p = 3142$ can be written as (1342).
3. $p \in S_4$ given by $p = 3241$ can be written as (134)(2).

While the cycle decomposition is unique, there is more than one way to denote the cycles. A canonical way to do this is by writing the greatest element of the cycle first, and then ordering the cycles in increasing order of their first elements. So the examples above can be written as

1. (2)(31)(645).
2. (4213).
3. (2)(413).