Algebra - I
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

One feature of elements in the group is their *order*. Suppose you have a group G and you have an element g in G, then consider the sequence $g, g^{2,} \ldots,$ where by g^2 I mean $g \cdot g.$ That is an infinite sequence of elements in the group g and there are two cases: either these are all distinct or not distinct.

In the first case we say that g has infinite order, in the second case we say g has finite order. When it has finite order we define its order to be the smallest nonnegative integer k, such that $g^k = id.$ We know such an integer exists since we know that $g^k = g^l,$ for some l>k; we can rewrite this as $g^{l-k} = id$ using cancellation we get that identity is equal to g of l minus k. So, there exist a smallest integer r, such that g^r is the identity. The simplest example is if you take the identity element of the group itself, then $id^1 = id$. So, this is order 1. But let us look at slightly more interesting cases,

Example 1.
Let us take the group G = Z/4Z. What are the orders of the elements here ?

	^1	^2	^3	^4
0	0			
1	1	2	3	0
2	2	0		
3	3	6= 2mod 4	5= 1mod4	0

So, what is the order of 0? Well 0 is the identity element of this group we already know that its order is **1**.
What is the order of 1? So we have 1, then 1 squared (note we are using the additive notations so 1 squared is 1 + 1); 1 + 1 + 1 that is 3 which is not zero in Z/4Z, when you take 1 + 1 + 1 + 1 that is 4 which is 0 in the group. So the order of 1 is **4**.
Now what do we do with 2 then? 2, 2 +2- which is 0. So, here the order is **2**
For 3 we will have 3, 3+3=2 mod 4, 3+3+3=1 mod 4, 3+3+3+3= 0 mod4. So, 3 has order **4**.
So, Z/4Z has 4 elements, one of which has order to another has order 1, one of order 2, and 2 elements of order 4.

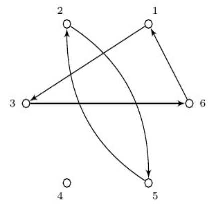
Now, I am going to talk about *conjugacy* of elements in groups. So, let G be a group and given two elements $g, g' \in G$, we say that $g \sim g'$ if there exists u in G such that $g' = u g u^{-1}.$ I claim that this is an equivalence relation. So, to check that something as an equivalence relation, we need to check three things: **reflexivity**, **transitivity** and **symmetry**.

Let us check reflexivity. Given an element g, is g conjugate to itself? It is by taking u to be identity.

Is it symmetric. So, if g prime is conjugate to g, then there exists u in G such that $g' = u g u^{-1}.$ But we can write this as $g = u^{-1} g' u.$, but $u = (u^{-1})^{-1}.$

To see that g is transitive suppose we have $g' = u g u^{-1}$ and $g'' = v g' v^{-1}$, and substituting we have $g'' = uv g v^{-1} u^{-1},$ and noting that $(uv)^{-1} = v^{-1} u^{-1},$ we see that it is transitive.

Example 2.
To understand order and conjugacy in the symmetric group we need to understand elements in terms of what is called the *cycle decomposition*. Suppose you have a permutation $w = 356421.$ I will think of the action of w on the elements [6]. So, w takes 1 to 3, 2 to 5, 3 to 6, 4 to 4, 5 to 2 and 6 to 1.



When you draw it like this what you see is that there are 3 cycles in w. We have (6, 1, 3), then we have another cycle which is (2,5) and finally, you have (4) which is also called a fixed point.
The *cycle type* of w is the lengths of the cycles of w written in weakly decreasing order. So, in this case there are three cycles. Their sizes are 1 2 and 3 and we write that in decreasing order we get 3 2 1. So the cycle type of w is 321.

More generally given a permutation w, $(i_1, i_2, .., i_r)$ is called a cycle of w if $w(i_1)=i_2, w(i_2)=i_3, \ldots, w(i_r)=i_1$.
Notice that there is some ambiguity in how we write this cycle. We can write the cycle (1,3,6) written as (3, 6, 1) or (6,1,3).

Now, let us see how we can read off order and conjugacy from the cycle decomposition of a permutation. Suppose w is a permutation and it has cycle decomposition $C_1, C_2, \ldots, C_l$. So, it has l cycles what is the order of w? Let us just start with a simpler example.

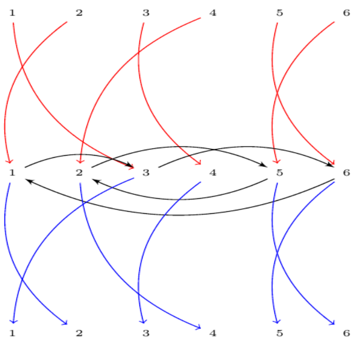
Example 3.
Suppose w is the cycle (123456): 1 goes to 2, 2 goes to 3, 3 goes to 4, 4 goes to 5, 5 goes to 6 and 6 goes to 1. If you look at w squared: it will take 1 to 3, 2 goes to 4, 3 goes to 5, 4 goes to 6, 5 goes to 1 and 6 goes to 2.
We want to know whether w squared is the identity or not. Well to check that is very easy: w^2 of 1 is 3, w^3 of 1 is 4 and so on w^5 of 1 is 6. So $w, w^2, w^3, .., w^5$ cannot be the identity element because none of them take 1 to 1, but w^6 of 1 is 1. You can check that w^6 of i is i for all i in [6]. So, the order of w is 6.

If $(i_1, i_2, \ldots, i_r)$ is a cycle of w, then $w^k(i_s)=i_s$ for all s in [r] if and only if k is a multiple of r. So, if w has cycle decomposition $C_1, C_2, \ldots, C_l$ where $\lambda_1, \lambda_2, \ldots, \lambda_l$ are the lengths of these cycles, then $w^k = id$ iff each of $\lambda_1, \lambda_2, \ldots, \lambda_l$ divides k. The least such integer is the lcm of $\lambda_1, \lambda_2, \ldots, \lambda_l$.

Theorem 1.
If $w \in S_n$ has cycle type $(\lambda_1, \lambda_2, \ldots, \lambda_l)$ then $o(w) = lcm(\lambda_1, \lambda_2, \ldots, \lambda_l)$.

So returning to the permutation w=(136)(25)(4), its order is 6.

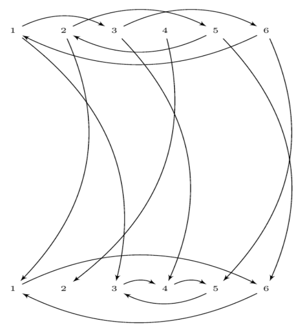
Example 4.
Now, let us try to understand conjugacy of elements using cycle type. Let w = 356421 and u is 241365 so u inverse is 314265. We need to figure out what it does to various elements of the set 1 to 6.



So by following the arrows (in the order red-black-blue) we find that $uwu^{-1} = (152)(46)(2)$.

So, what we see is that if $(i_1, i_2, \ldots, i_r)$ is a cycle of w then $(u(i_1), u(i_2), \ldots, u(i_r))$ is a cycle of $u^{-1}wu$ Conversely, suppose w, w' have the same cycle type then.

Example 5.
Let w be as before and let $w' = (16)(345)(2)$. The u we choose must map elements of cycles of the same length bijectively:



which yields u=314265. Note that this u need not be unique- it depends on a choice of bijection for each cycle.

Exercise 1.
How many such elements u exist in this case? How many exist for a permutation which has m_1 cycles of length 1, m_2 cycles of length 2, ..., m_r cycles of length r? (Hint: In this case we must first choose which a matching between cycles first and then choose an appropriate bijection between the elements of the matched cycles.)

Theorem 2.
Two permutations $w, w' \in S_n$ are conjugate if and only if they have the same cycle type.

Example 6.
What are the conjugacy classes in S_5 ?
We just have to write down all possible cycle types. The identity element has cycle type is **(1, 1, 1, 1, 1).**
The cycle types are all sequences of positive integers that sum to 5: in addition to the cycle type of the identity we have **(2,1,1,1),(2,2,1),(3,1,1),(3,2),(4,1),(5).**

To recapitulate:

- The order of an element g in a group G is the smallest nonnegative integer k such that $g^k = id.$ It may be finite or infinite.
- Two elements $g, g' \in G$ are said to be conjugate if there exists an element u in G such that $g = u^{-1} g' u.$
- Conjugacy is an equivalence relation on elements in a group.
- Every permutation can be written as the union of disjoint cycles. This is called its cycle decomposition. The lengths of the cycles in nonincreasing order is its cycle type.
- The order of a permutation is the lcm of the lengths of the cycles in its cycle decomposition.
- Two permutations are conjugate if and only if they have the same cycle type.