Algebra - I

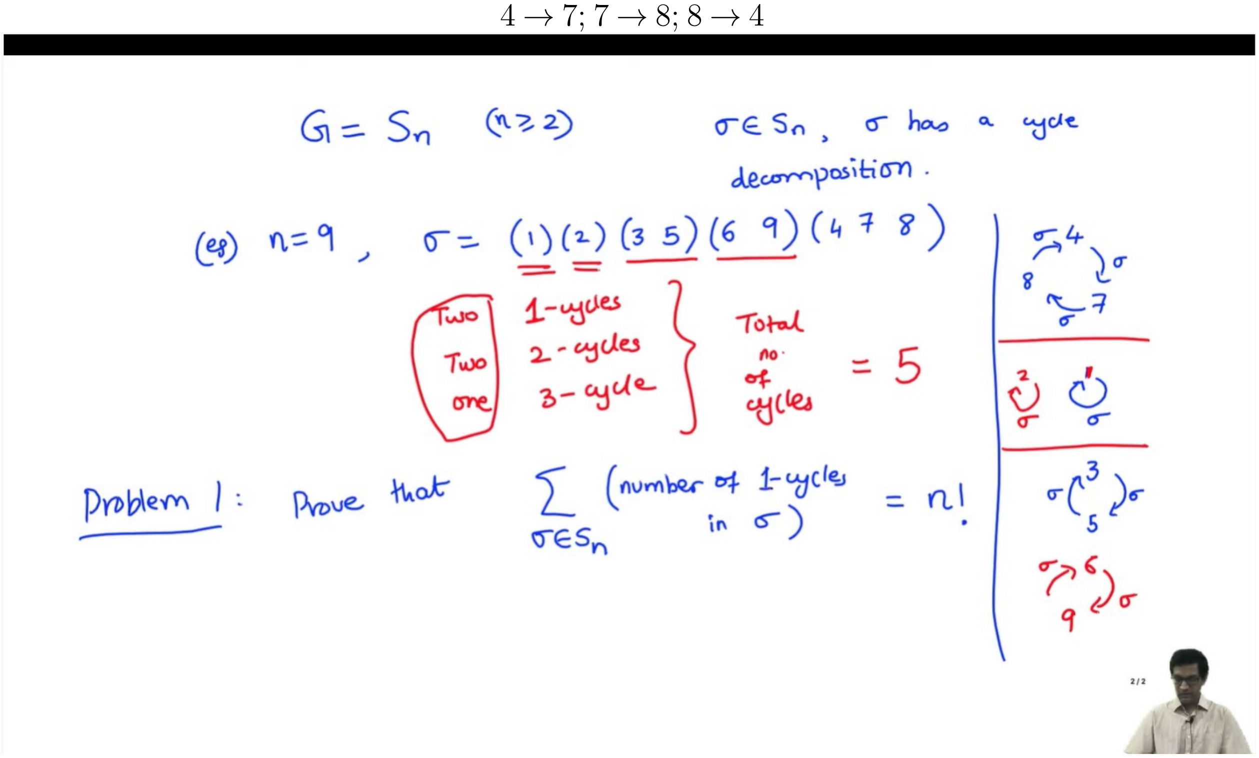
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

1. Lecture 20

[Problem Solving I]

Let us do some problems ok on groups and group actions and so on . So, here is problem 1 , so to state this problem let me first recall something about symmetric groups and cycle decomposition and so on. So, recall if I take the group G to be the symmetric group S_n , so n is let us say at least 2 symmetry group and if I take a typical element of S n I have a cycle decomposition right. So, σ has a cycle decomposition recall this means that you can write it as a product of disjoint cycles. So, let us maybe do it by example suppose $n = 9$. So, I am looking at S_9 and if σ say is the element it is a product of (1)(2)(35)(69)(478) ok. So, this is a permutation of the numbers 1 through 9 and the cycle decomposition this says that for example that (478) form a 3 cycle in other word σ maps 4 to 7. So, this is what σ does it maps 7 to 8 and it maps 8 back to 4 ok.

$$4 \to 7; 7 \to 8; 8 \to 4$$



So, the element 1 is mapped back to itself and so on ok. So, there are some 2 cycles as well 3 goes to 5, 5 goes to 3 .

$$3 \to 5;\ 5 \to 3$$

So, recall this is what decomposing permutation into cycles means . Now here is what I want to look at I want to sort of study the lengths of the cycles or maybe for a start let us look at how many 1 cycles does do the various elements of S_n have ok. So, what do we mean by a 1 cycle . So here for example this particular example of σ this particular σ has two 1 cycles ok. So, it actually has two 1 cycles ok by 1 cycle I mean the length of the cycle is 1. In other words this 1 is really a fixed point of sigma, σ maps 1 back to itself ok it actually has two 2 cycles as well. So, this has two 2 cycles ok which are (35) and (69) . And it has one 3 cycle which is 4 going to 7, 7 going to 8, 8 going to 4 ok. So, this is the 3 cycle there are two 1 cycles and there are two 2 cycles ok .

So, in particular what is the total number of cycles if you wish? So, total number of cycles total number of cycles is 5 in this case ok, so 2 plus 2 plus 1 ok. So, here is the first problem, so this was all by way of preliminary. So now, let me state the problem . So, let us consider the following sum. So, prove that if you take the sum over all elements of S_n I take the number of 1 cycles in sigma, this sum will always give me the answer n! ok.

$$\sum_{\sigma \in S_n} (number\ of\ one\ cycles\ in \sigma) = n!$$

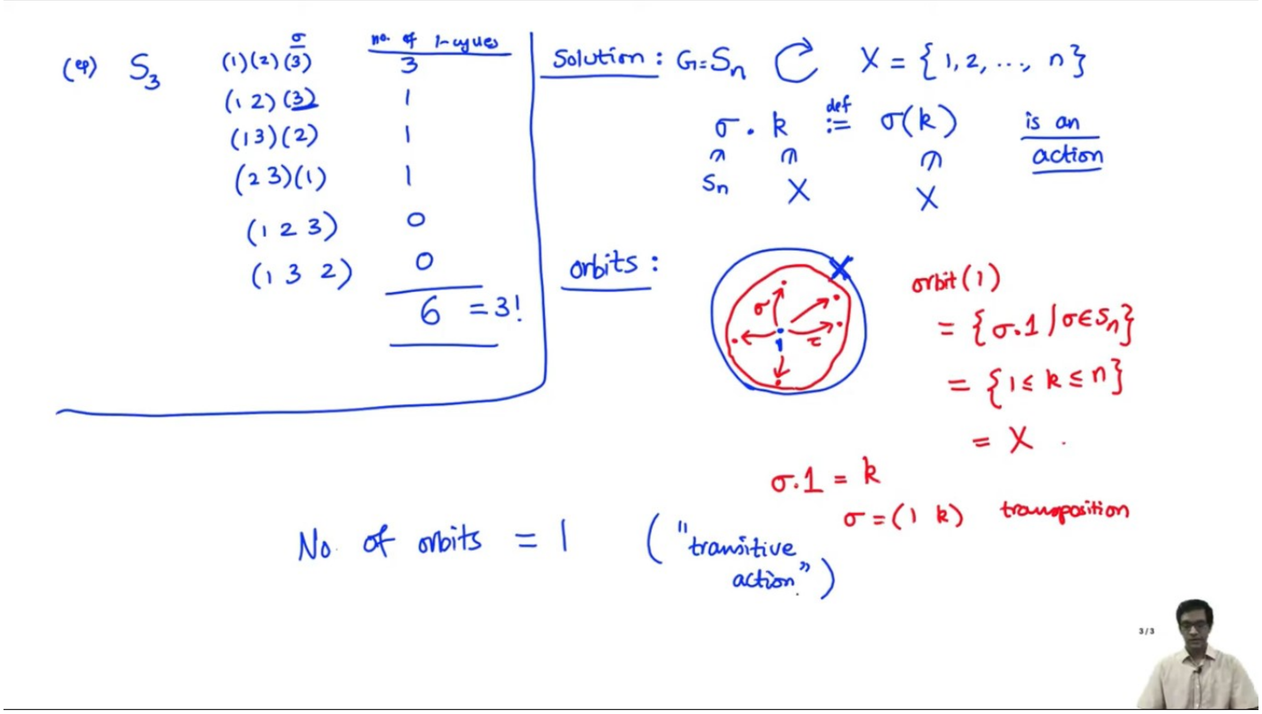
So, the sum of the number of 1 cycles of σ sum over all elements σ ranging over S_n gives me the order of the group S_n which is n! ok. So, let us check this out in some easy simple cases. So, example suppose I just look at the symmetric group

$$S_3 = \{(1)(2)(3), (12)(3), (13)(2), (23)(1), (123), (132)\}$$

and let me just write out all the element σ. So, here is σ , so this is the identity element one going to 2 going to 3 I am sorry 1 2 and 3 each going to itself . Here are the transpositions which only permute 2 of the elements and leave the third one fixed and there are these two 3 cycles ok.

So, there are 6 elements of sigma, now let us tabulate the number of 1 cycles ok how many 1 cycles do we have in each. So, here there are 3 1 cycles ok this guy the next one has only 1-1 cycle which is just a singleton 3 is likewise these 2 also have only 1-1 cycle, these 2 permutations the last 2 guys do not have any 1 cycles because. In fact, it just has a single 3 cycle ok, so let us add all these up so that is 3 plus 3 which is 6 just exactly 3! ok. So, this is an an instance of of this problem this example if you take n equals 3 you do actually get 3! ok. So, let us see how does one prove statements like this. Often many of these problems can be rephrased appropriately as a problem about group actions ok.

So, at this point I would encourage you to sort of you know spend some time trying to work out the solution on your own . But let me also tell you how to do this. So, if you do not succeed here is the solution which you can look at maybe for hints or for the entire solution . So, here is the here is the idea. So, let us take this group S_n and let us look at a following natural set on which it acts ok. So, this is the set of all numbers from 1 to n ok. So, recall this group G acts on this set X in the following natural way. If I take an element $\sigma \in S_n$ how does it act on element k from the set X , well k since it is some element from $\{1, 2, 3, ..., n\}$ and σ being a permutation of the numbers $\{1, 2, 3, ..., n\}$, σ will act on k and give me some other number between $\{1, 2, 3, ..., n\}$ right.

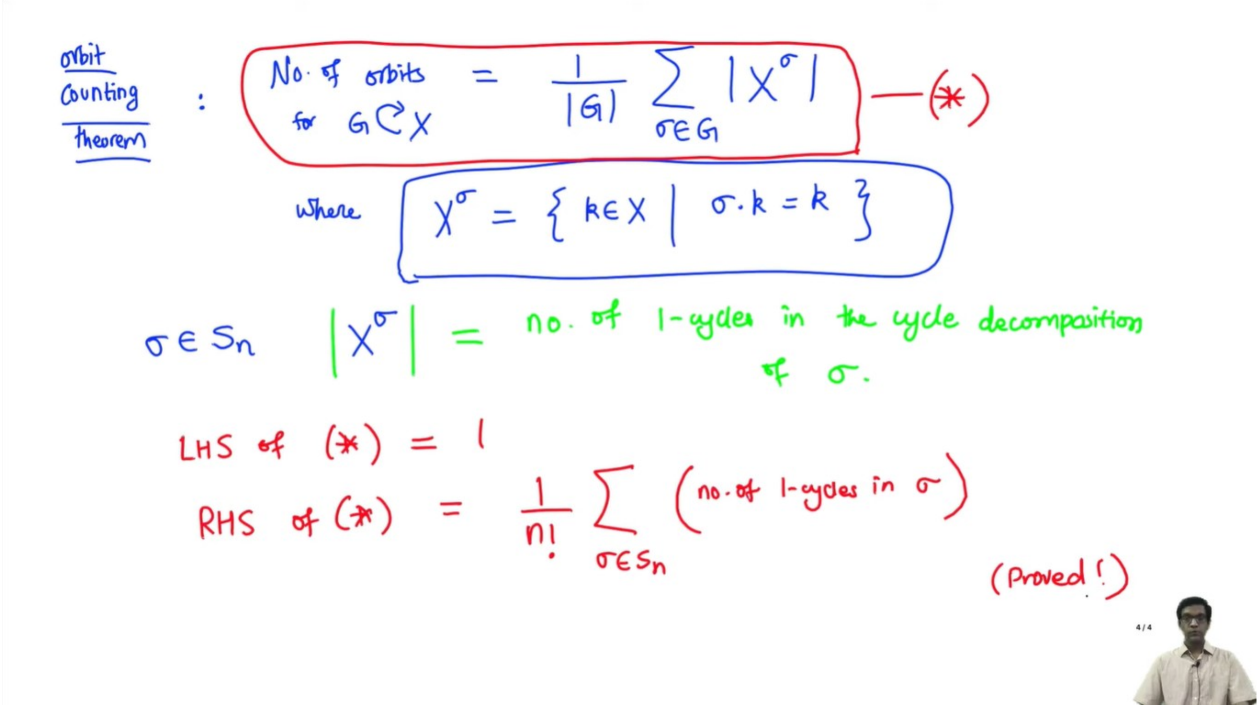


So, here is the definition you just define. So, definition I define σ acting on k to just be

$$\sigma \cdot k := \sigma(k) \in X$$

ok this is the definition ok and of course that is also an element of X ok and it is easy to check this is an action, so this is an action . So, sometimes called the defining action of this group Sn, some sense the group is it occurs naturally as you know the set of all possible you know permutations of the set ok. Now , now let us do the following let us look at this orbit counting statement ok. So, we have the theorem which tells us how to determine the number of orbits for a for an action of a group. So, let us study the orbits first. So, let us first ask ourselves what are the orbits of this action look like ok . If you just spend a couple of minutes you will realize that in fact there is only 1 single orbit here ok.

So, recall this is the set X . So, what is the orbit mean ok, how do I construct orbits? For example, I take 1 single element of X say the element to 1 and the orbit of this element 1 will just mean I have to act every possible group element on 1 and collect together all the answers that I get ok. So, I on 1 I act by various elements, so I act by some group element σ by some other group element tau and so on. So, I keep acting on 1 by every possible group element and I will get some elements of my set the collection of all these elements is what is called the orbit of my 0.1 ok. So, let us write that down the orbit of the element 1, by definition is just σ acting on 1 for all σ ranging over S_n ok. But notice you can always find a permutation which takes the number 1 to any other number between 1 and n ok. So, by suitably constructing $\sigma's$ I can get every element k here. So, this will give me every number $1 \leq k \leq n$ ok, in other words this is just the the whole set X itself ok and what is the easiest σ which maps 1 to k. So, if I want an element σ which takes 1 and maps it to k, well I can take just the transposition $(1k)$.



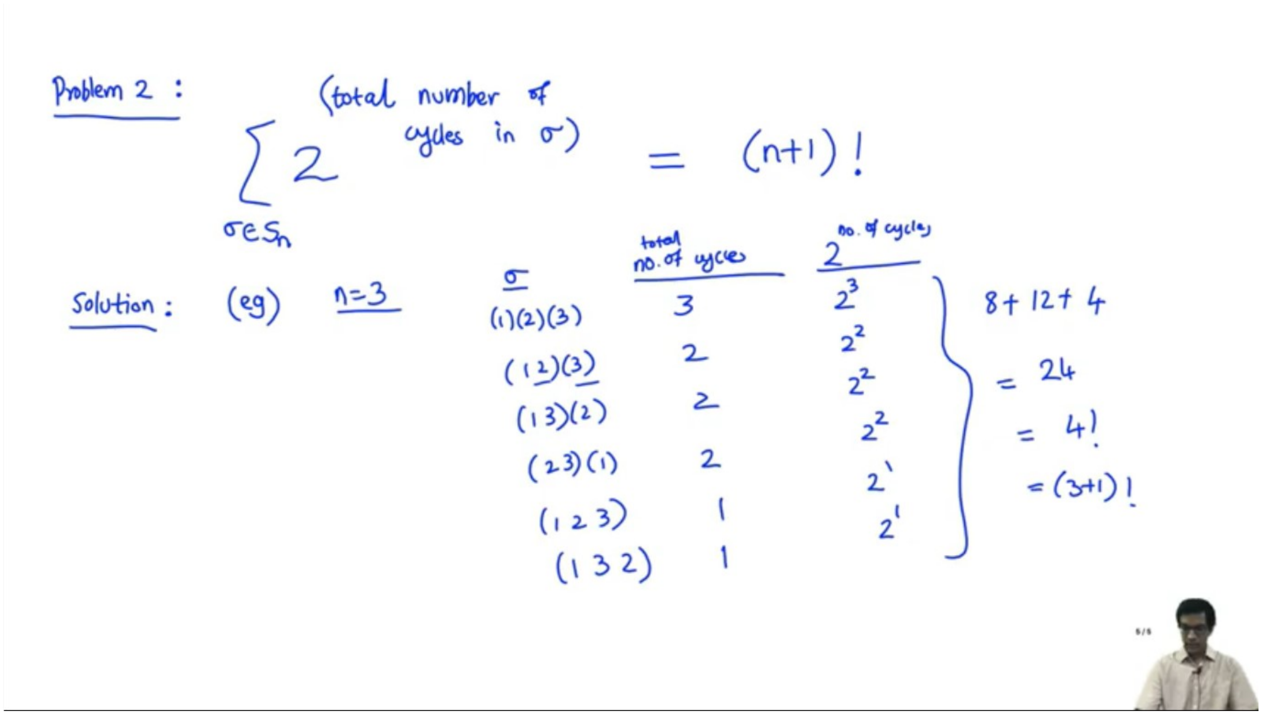
So I can take for example, the element $(1k)$ and leaving all the others fixed. So, there is just the transposition which maps 1 to k and and leaves all the other numbers fixed, this permutation of course takes the number 1 and maps it to the number k ok. So, this is an example of one such element. So, it is clear that the orbit of 1 is in fact the entire set X here ok. So, in particular it means that the number of orbits . So, the number of orbits for this particular action is just 1 ok. So, such an action is sometimes called a transitive action , in which there is only 1 orbit in other words every element of the set can be mapped to every other element of the set by some action of some group element ok. So, we have determined the number of orbits to be 1.

So, now let us apply our orbit counting theorem. So, what does the orbit counting theorem say orbit.

$$No\ of\ orbit\ for\ G\ acts\ on\ X = \frac{1}{|G|}\sum_{\sigma\in G}|X^\sigma|$$

So, this is a number of orbits for the group action G on X ok it was given by this. So, recall this is also called burn sides lemma and so on. Where $X^\sigma = \{k \in X | \sigma \cdot k = k\}$ is the fixed point set meaning it is all those elements of X which are mapped to themselves.

So, $\sigma(k) = k$ ok this all elements of the set which are mapped to themselves by sigma, the fixed element of the group ok. Now this set the fixed point set what does it mean? So, if I pick some element $\sigma \in G$ my group $G = S_n$ here, what is the fixed point set mean? Well observe that you know what are the fixed points of a permutation well those are exactly the one cycle. So, let us go back up look at this this picture of σ that we had. So, observe that the if if you want a point k which maps to itself under σ right, that is what a fixed point mean σ k equals k then these are the only 2 options. So, these are the only 2 fixed points the numbers 1 and 2 are the only fixed points for this particular σ ok. So, observe in this example X^σ the fixed points are just the numbers 1 and 2. None of the other numbers can



be fixed points for example, when you see the cycle decomposition it becomes clear 4 cannot be a fixed point because, σ maps 4 to the next element in the cycle ok and that element is not itself.

Because the cycle has length at least 2 , same thing here 3 cannot be a fixed point because σ takes 3 to whatever the next element of the cycle is ok and so on. So, the only way you can get fixed points if is if that element occurs as part of a 1 cycle ok. So, what does that mean we have proved the following that. In fact, the number of fixed points therefore is the same as the number of 1 cycles ok. It is the number 1 cycles in the cycle decomposition of σ and now we are more or less done because all we have do is just look at this this statement here ok put everything together.

So, observe if we take this statement let me call this equation star. So now I i just look at the following thing the left hand side was the number of orbits which we know is 1 . The right hand side is according to what we just said it is 1 by the cardinality some overall group elements of the fixed point set which is just the same as the number of 1 cycles ok. And now we are done because these 2 things are equal and that is exactly what we had to prove ok. So, proved proved whatever we needed to prove which is the statement appear that the number of 1 cycles in σ summed over all group elements gives me $n!$ ok. So, that is an application of group action. So, let us do one more along the same lines. So, here is problem 2 ok. Now this this time it is not the number of 1 cycles that we will look at, but rather we will just look at the total number of cycles ok. So, now I am going to just say let me look at the total number of cycles , total number of cycles in the cycle decomposition of σ ok. So, what does that mean let us go up again , here for instance the total number of cycles was 5 ok. So, I i do not care what the individual lengths of the cycles are, I just want to know how many total number of cycles there are ok.

So, I take the total number of cycles, but I do something slightly different here. I look at 2 raise to the total number of cycles ok 2 to the power of total number of cycles summed overall elements of the group S_n. Now I claim it gives me $(n+1)!$ not n! anymore, but rather $(n+1)!$ ok. Again an interesting sort of statement, again please try this on your own . But here is the solution nevertheless . So, as before you know in all these things let one should always try these out on some simple examples. So, let us do the same example as before which is the case of $S3$ and let us write out all the the element σ as before I have

$$S_3 = \{(1)(2)(3), (12)(3), (13)(2), (23)(1), (123), (132)\}$$

there are 6 elements.

Now, in each case let me say how many total number of cycles, so this is the total number of cycles . So, here there are 3 of them here I have 2 cycles this one and this one here again 2 cycles 2 cycles these 2 have 1 cycle each ok. But remember I have $2^{(totalnumberofcycles)}$ right. So, that is for the first guy 2^3 the second guy 2^2 , 2^2 , 2^2 , $2, 2$ ok. So, let us add all these numbers up they are all various powers of 2. So, I have $8 + 12 + 4 = 24$. So, that gives me a 24 ok 244! is actually 4!, now it is not 3! anymore it is $(n + 1)!$ ok.

So, that is the that is the next interesting fact about the number of cycles which occur in the various cycle decompositions of elements of of the symmetric group ok. Let us prove this again a proof by group actions.

So, here is the solution ok. So, as before let us look at the group $G = S_n$ and it had this defining action it acted on the set $X = \{1, 2, 3, ..., n\}$ which was 1 to n . But we have encountered this following construct when a group acts on a set it also acts on all subsets of that set ok. So, now because I have this action of G on X it implies I can also consider another action of the group G on the power set of $P(X)$ ok. So, what is this the power set of X just means the set of all Y subset of X ok,

$$P(X) = \{Y|Y \subseteq X\}$$

maybe we should say a set of all Y where Y ranges over the subsets of X ok. So, the power set of X is well I also include the empty set here.

So, we have we have seen this before, I have a natural action. What is the action? If I take an element $\sigma \in G$ if I take a subset $Y \subseteq X$ the action of σ on Y is just defined to be the the element wise action. So, I take σ and I act on k for every k coming from the subset Y ok. Now, when I do this what I generate is again some new subset of X right potentially a different subset of X ok. Now we had also seen a finer thing here that this subset $|\sigma \cdot Y| = |Y|$. So in fact, you can also say that the there is an action of the group G on subsets of X of a certain fixed cardinality also if you want ok.

In this case we will not need that that finer distinction, we will just look at the action of G on the entire power set ok. But let us make this observation nevertheless it is an important observation which we will need, that the cardinality of σ acting on Y is the same as the cardinality of Y ok. Because when σ acts on k for every every $k \in Y$ it gives me distinct elements ok. So, this is an important property ok.

Now again let us do the same analysis as before let us understand what the orbits look like for this action and how many orbits there are. So, what are the orbits well the first thing to observe is that because, the cardinality of $|\sigma \cdot Y| = |Y|$, we certainly cannot you know we we we cannot change the number of elements in a subset by acting by some group element ok. So, this particular group action preserves the cardinalities of the subsets. So, let us define those subsets $P_d(X)$. So, what is

$$P_d(X) = \{Y | Y \subseteq X; |Y| = d\}$$

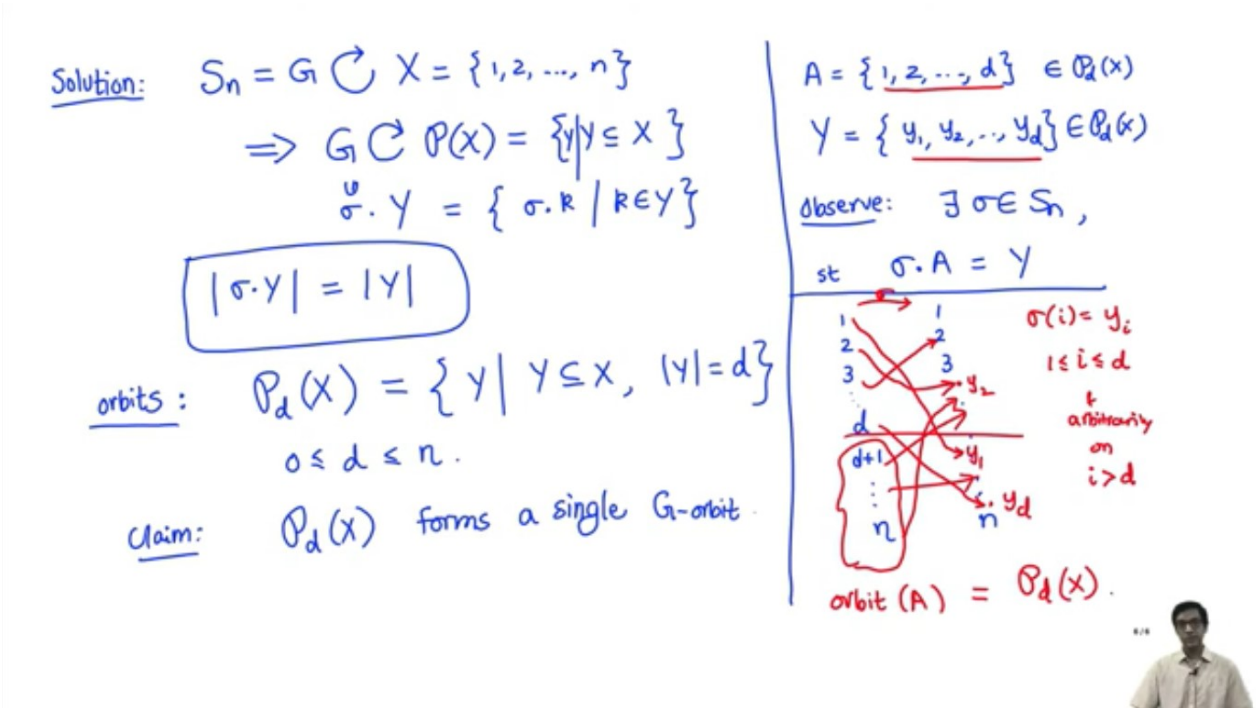
in this case this is just all Y such that Y is a subset of X and Y has cardinality d ok. So, what is d here d can be 0 and go all the way up to the cardinality of X , the cardinality of $|X| = n$ ok.

So, in order to understand the orbits I first construct these these elements Pd of X ok. So, these are subsets of a fixed cardinality. Now I claim that the set $P_d(X)$ is a single G orbit ok. So, here is the first observation we make that $P_d(X)$ this subset of $P(X)$ forms a single G orbit ok. So, let us prove this. So, what is this forms a single G-orbit mean? I have to show that given any two subsets of say cardinality d , I can map one to the other by means of some group element ok or let me sort of do a simpler thing. So, let me take the the subset $A = \{1, 2, 3, ..., d\}$ ok let me call this subset A. So, consider the subset 1 2 3 till d ok. So, this is a particular element particular subset in $P_d(X)$ sort of a special guy the first d consecutive numbers. Now, let me take any other subset of of cardinality d. So, let me write out the elements let us call Y as. So, what are the elements of $Y = \{y_1, y_2, ..., y_d\} \in P_d(X)$ ok. There is some arbitrarily written out elements I just label them as $\{y_1, y_2, ..., y_d\}$ in any way I care and now let me claim that I can construct.

So now, observe the following that I can construct an element in my group S_n there exists $\sigma \in S_n$, sense such that, when $\sigma \cdot A = Y$ ok. And how do I construct this this sigma, well what is it that I need to do how do I construct σ. So, I sort of have some, so here is how I construct σ $d+1, ..., n$ remember σ is some permutation of the numbers 1 through n right. So, how do I want it to be $1, 2, 3, .., n$? So I need a construct σ, now so that is what I am going to. So, this this map now is going to be σ. So, I already know something that I want σ to satisfy ok, when σ acts on these d elements and suppose to produce these d elements right. So, many different ways of doing it here is how I could do it easily, I take σ which takes one and maps it to y_1 ok. So, I scan my right hand side somewhere there is this number y_1 right.

So, I I define σ like this σ sends $1 \rightarrow y_1$ ok I look through my list somewhere there is y_2 σ maps $2 \rightarrow y_2$ ok it maps $3 \rightarrow y_3$ whatever that may be and so on ok. So, the first d numbers I map it to $\{y_1, y_2, ..., y_d\}$ in that order ok. So, define σ like this σ should map $i \rightarrow y_i$ for $1 \leq i \leq d$ ok. And for the remaining numbers from $d+1, ..., n$, I do not really care ok and just map it arbitrarily. So, that it is it is still a permutation ok and define it arbitrarily on $i > d$ ok. When I say arbitrarily of course, the final n product must still be a permutation ok. So, I have to define it to be some bijection, but all I have to do is $\{y_1, y_2, ..., y_d\}$ are already gone they are taken because they are the images of 1, 2, 3,..., d and so the remaining $n-d$ numbers which will be there on the right hand side and then I have the these remaining $n-d$ numbers $d+1, ..., n$. I sort of just map these remaining guys to those remaining guys in a 1 to 1 onto fashion. So, some arbitrary bijection of of those two sets ok. So, I hope it is clear that if I take any subset Y of cardinality d , I can always find a permutation σ which will map $A \rightarrow Y$ ok. Now what is does this mean? It means that the orbit of A is the entire set $P_d(X)$. So, this just tells me that if I take this special set A and I look at it is orbit well that is everything $P_d(X)$ ok.

So, $P_d(X)$ forms a single orbit and observe that if I take subsets from $P_d(X)$ and $P_{d'}(X)$ you know subsets of 2 different cardinalities. Then as we have said already I cannot find a



group element which maps one subset here, I mean I which maps the subset of carnality d to A subset of cardinality d' where d' is different from d ok.

So, what this this argument entails is what it implies, therefore is the following conclusion that the G-orbits for the action of this group S_n on the power set of $P(X)$ are precisely the following $P_0(X) = \emptyset$,this is the empty set $P_1(X), ..., P_n(X) = \{X\}$ is the singleton comprising the empty set . ok. So, these are exactly the the the orbits for the action of this group.

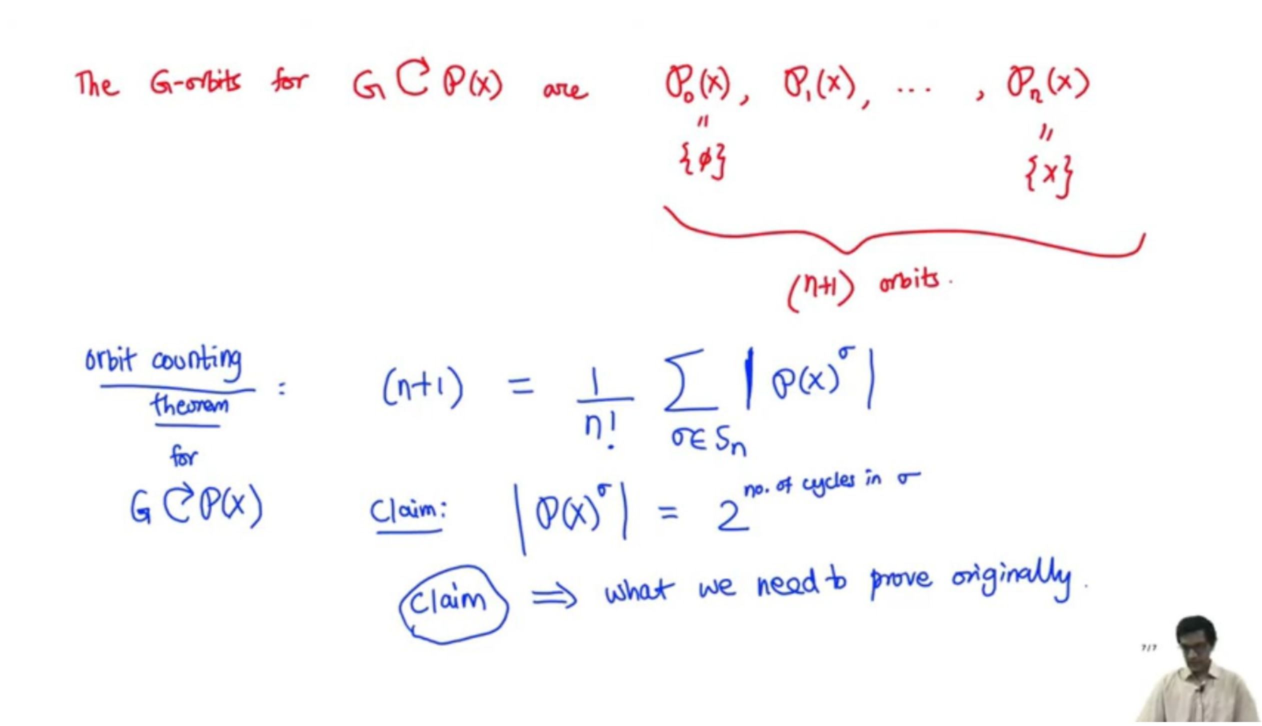
Now, how many orbits do I have exactly $n+1$, so $n+1$ orbits ok. Now again let us use our orbit counting theorem. So, orbit counting theorem says that the total number of orbits which in this case is:

$$(n+1) = \frac{1}{n!} \sum_{\sigma \in S_n} |P(X)^{\sigma}|$$

So, I have just applied the orbit counting theorem for the action of the group S_n on the power set of $P(X)$ ok, when I do that this is the equation I deduce from that ok. Now all that remains is to understand what this this right hand side looks like and I claim that that

$$|P(X)^{\sigma}| = 2^{(no.\ of\ cycles\ in\ \sigma)}$$

So, once this claim is established the the problem is done, because you know as you can see this is the sum would then become the sum of $2^{(no.\ of\ cycles\ in\ \sigma)}$ and I can take this $n!$ over to the other side $n!(n+1) = (n+1)!$ ok. So, if this this claim is done then I am done ok, claim implies what we need to prove prove originally ok . So, the problem is done provided we prove the claim ok. So, let us try and understand why this is true. So, I claim that if I fix a certain σ with a certain cycle structure then the the the number of fixed points for the

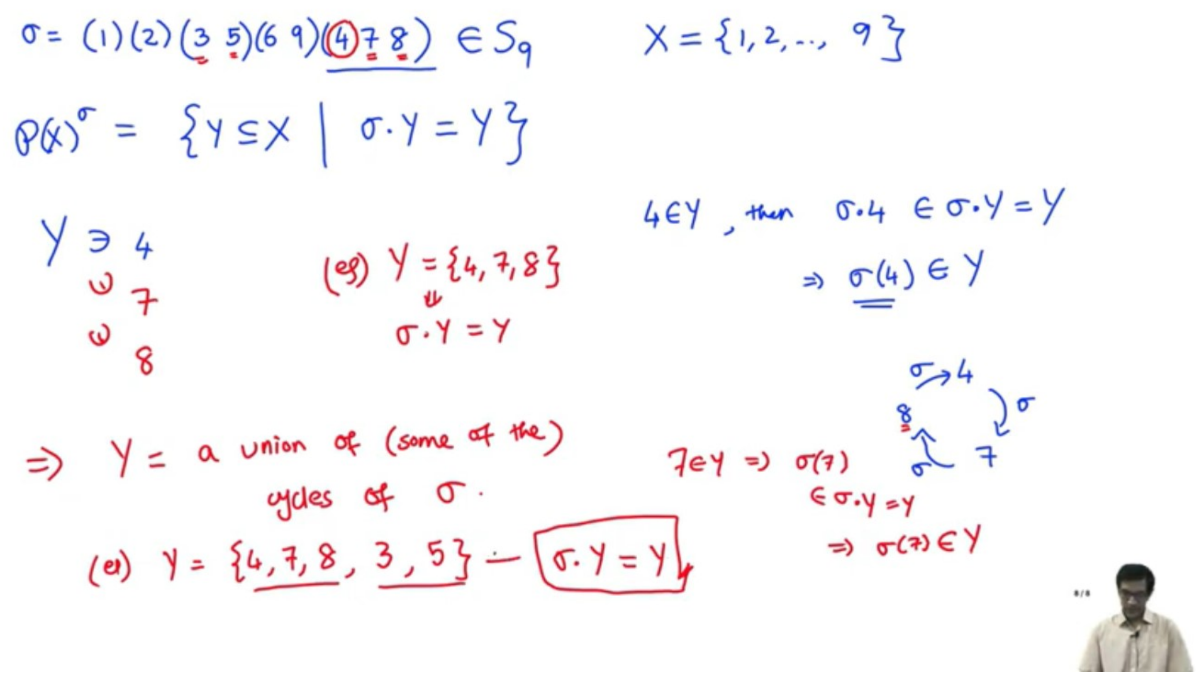


action of σ on $P(X)$ is exactly this number 2 to the number of cycles. So, let us sort of do this by by example maybe for a start.

So, suppose I take $\sigma = (1)(2)(35)(69)(478)$. So, this was a permutation inside S_9. So now I am going to ask suppose I take $X = \{1, 2, 3, ..., 9\}$ then how many subsets of X are fixed under this action of σ ok. So, I want to understand $P(X)^\sigma = \{Y \subseteq X | \sigma \cdot Y = Y\}$ which is what set of all subsets Y of X , such that σ acting on Y should give me back Y ok. So, let us see what are the possibilities for for Y , what can it what can be the elements of Y ok. So, let us see suppose I take Y to have some some number right, Y should have at least one of these I mean Y is non empty it must contain some number.

So let us say for a start, suppose Y has the number of 4 ok let us try to understand suppose $4 \in Y$ ok. Now what what what do we conclude from that? So, observe when I act $\sigma \cdot Y = Y$ ok. So, if $4 \in Y$, then $\sigma(4) \in \sigma \cdot Y = Y$. So, we conclude that therefore σ acting on 4 which is σ evaluated on the number 4 this must also be an element of $\sigma(4) \in Y$ ok. So, what does that mean $\sigma(4)$, now remember this is part of this 3-cycle here. So, if 4 is there in Y then we conclude that $\sigma(4)$ is also there in Y ok. So, 4 7 8 so this is all $\sigma(x)$ ok. So, what we have concluded is if 4 is in Y then the next guy in the cycle which is 7 must also be in Y ok.

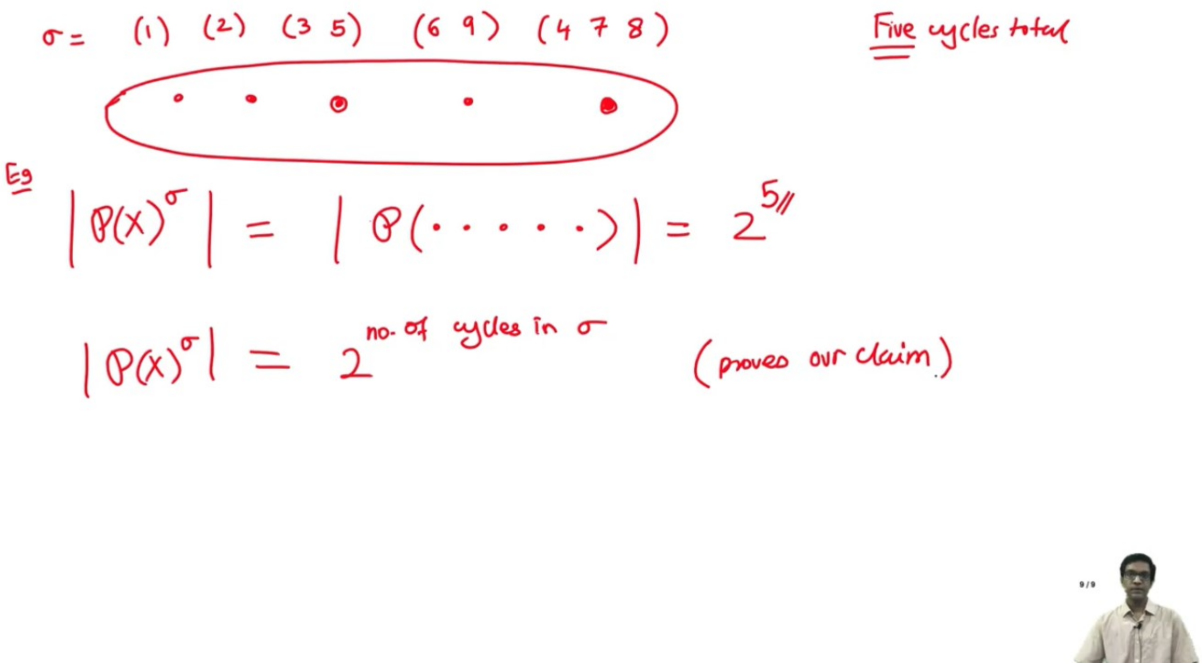
Now observe we just repeat the same argument with 7 in place of 4 ok. So, 7 belongs to Y means by the same token σ acting on 7 will belong to σ acting on Y sorry σ acting on y which is y again , so this implies that $\sigma(7) \in Y$ and $\sigma(7) = 8$. So, we conclude that 8 must also belong to Y ok. So, what this means is that so this this argument now establishes the following, if one member of a cycle so 4 in this case if 4 is in Y that automatically forces the other members of the cycle to also belong to Y ok. So, what that means is that Y is therefore a union of some of these cycles, it is a union of some of these cycles of σ not all of them need need to appear.



So for example, Y equal just 4 7 8 is would certainly be a fixed point. Suppose I take Y only to have the numbers 4 7 and 8 , then observe that $\sigma \cdot Y = Y$ so this this is enough. So, I can only take those 3 numbers and I will certainly get something that is a fixed point ok. Or what is another example I could take a union meaning here is another example of a fixed point, I can take the elements 4 7 and 8 . Then maybe I can take the element 3 as well, but if I take 3, I am also force to take it is partner in the same cycle ok. So, I am supposed to also take 5 only if I do that can I have a chance of Y being a fixed point.

So, in this case let us see whether the set of 5 elements is in fact fixed 4 7 8, if I apply σ to those 3, I will just keep cycling through those 3 numbers; 3 and 5 when I apply σ to 3 , I get 5 , when I apply to 5, I get 3 ok. So, when I act σ to these to this set of 5 elements I get back the same set of 5 elements ok. I get get them in a different order maybe when I act on it, but I do not care I just want the final set to be the same ok. So, here is another example of a subset of these 9 elements such that σ acting on gives me back σ acting on Y gives me back Y ok so and so on. So, what this means is that in general how do I produce all these Y which are fixed points. Well this is just the collection of all unions of of some cycles of σ ok. Now what does that mean well let us just look at how do we see how many elements there there are therefore ok. So, what do I have I have the the following cycles. So, remember $\sigma = (1)(2)(35)(69)(478)$.

So, how do I find Y well out of these 5 cycles totally so there are 5 cycles total . So, out of these 5 I can choose any subset of the 5 ok. So, I have 5 possibilities. So, let me represent each cycle by a dot there are 5 dots ok, there are 5 possible cycles and out of these 5 I can choose any subset ok. For example, I can choose only this this last cycle, so then I will get 4 7 8 as my Y . If I choose this last cycle and this guy then the choosing those 2 cycles would amount to choosing the set $Y = \{4, 7, 8, 3, 5\}$.



The the subset of 5 elements, if I do not choose any of these dots that is like saying I do not choose any of the cycles in other words Y is the empty set or if I choose all 5 dots it means I am choosing all 5 cycles in other words all 9 numbers ok. So, it is clear therefore that the the possible Y is that you can have the set of fixed points. What is the cardinality?

Well it is just the cardinality of the subsets of these these 5 dots for example ok and how many well that is just the power set of this set of 5 dots if you wish ok. So, in our example so I am I am just trying to say what it is in this example well in this example this is nothing but the same cardinality as the power set of the set of 5 dots ok.

It is just all possible ways of choosing some sub collections of these 5 dots . But remember the power set of a set has cardinality 2 power the number of elements in that set ok. So, in this case this is 2^5 and remember this 5 where did this come from well it is because there are 5 total cycles ok. So in general therefore the same argument in general proves the following that this is just 2 power the total number of cycles in σ ok and that that establishes our claim. And we are done proves our claim and thereby the the original statement that we wanted to prove ok .