NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract Group Theory
Module 05
Lecture 28 –"Symmetric groups III"
PROF. KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE
(Refer Slide Time: 00:25)

But now what about products of disjoint cycles, what about the order of product of disjoint cycles? And this is dealt by next proposition. It says that if sigma is an element of symmetric group has cycle decomposition, let us say sigma equals sigma 1, sigma 2 up to sigma k. So remember cycle decomposition always assumes that the cycles are disjoint cycles.
And let us say sigma 1, sigma i is a mi cycle. So in sigma 1 is a cycle of length m1, sigma 2 is a cycle of length m2, sigma k is a length of mk. Then order of sigma is lcm, least common multiple of m1, m2, mk.

(Refer Slide Time: 01:57)

So proof, so first of all, LCM stands for least common multiple. So now we have in the previous proposition showed that if you have a single cycle its order is the length of that cycle, so if it is a k-cycle its order is k. Now I am, in the new proposition, I am telling you if you have a cycle decomposition into a product of k cycle, which are disjoint, that is important, and then the order of the product is the lcm of the individual orders. Remember order of sigma i is mi, and the order of sigma is lcm of mi. So this is very easy to prove.

So by the previous proposition, let us quickly prove this, by the previous proposition, order of sigma i is mi, let us keep this in mind, for i from 1 to k. So order of sigma is mi, because sigma i is an mi cycle. So it has order mi.

So let M be the lcm ,so for simplicity let capital M be the lcm of m1 to mk. Now what is sigma power m. Let us compute sigma power m. This is sigma 1, sigma 2, up to sigma k power M. So remember this means I am doing sigma 1, sigma k, sigma1, sigma k, sigma1, sigma k M times. So in general permutations do not commute with each other, but disjoint cycles do. So you can sigma 1, sigma k is sigma k, sigma 1. Because they are disjoint cycles.

Because they are disjoint cycles, we can interchange them, and in a group we can apply associativity law, so we can remove the brackets first. Sigma k and sigma 1 can be interchanged. And then you reorganize all of them and put all sigma 1 to the beginning, so you get sigma 1 power M. Then you put all sigma 2s , basically commutativity of these sigma i means that you can arrange them in any order.

I will put all sigma 1s, there are M of them, then all sigma 2s, then all sigma 3s, and finally all sigma ks, so I can write this sigma power M as this. But now M is the LCM of mi, small mi, so order of sigma 1 is m1, and m1 divides capital M, because capital M is the LCM of m1 through mk, so in particular m1 divides M. This implies, sigma 1 power M is identity. This is something we have seen in detail in various situations, if you have order times something, power of that will be identity.

Similarly, sigma 2 power M is also identity because m2 also divides M, m3 divides M so that is e, so everything is e. So sigma power M is e. This means, order of, remember order of sigma is supposed to be M. So we have to prove that order of sigma is M. So in other words, the least positive integer d such that sigma power d is identity, is M. We have checked that sigma power M is identity. We now need to check that nothing smaller than M can make identity.

(Refer Slide Time: 06:19)

So suppose sigma power n is identity, by the same calculation above, so e is sigma power n, just like we calculated here, because sigma 1, sigma2, sigma k commute with each other, I can write sigma power n as sigma 1 power n , sigma 2 power n , sigma k power n. I can re-arrange them, so that all sigma1s comes first, sigma 2s come next, sigma 3s come next and finally sigma ks come next.

Now let us stare at this equation for a while, remember sigma 1, sigma 2, sigma k are disjoint cycles, so whatever index appears in sigma 1, does not appear in sigma2, does not appear in sigma3. But after applying, suppose i is an index appearing in sigma1, then so i does not appear in sigma 2, sigma 3, because sigma 1 is disjoint with sigma 2, i appears in sigma1, so it does not appear in sigma2 and doesn't appear in sigma3 and sigma k.

Now I claim that this implies i does not appear in sigma 2 power n also, sigma 3 power n also, sigma k power n also. Because remember sigma 2, when you apply to itself, it only talks about, deals with indices that originally appear sigma 2. In the previous examples when we proved to previous proposition, remember if we take (1, 2, 3, 5) as a cycle, its products with itself only involve the original indices that appear in sigma, in this example it is 1,2,3,5. So products will only involve 1,2,3 5.

Suddenly a new index cannot appear right, because sigma fixes an index powers of sigma continue to fix that index. So we don't have to worry about if i does not appear in sigma 2, i does not appear in sigma 2 squared. Sigma 2 power 3 , sigma 2 power n. So i only appear in, hence i only appears in sigma 1 power n, so i only appears in sigma 1 power n. May be it doesn't appear in that also, because may be it is fixed by I, but it cannot appear in sigma 2 power n and sigma k power n.

So now e fixes i that because e is the identity element, so sigma n fixes i, because sigma power n is e, I am assuming sigma power n is e for some n. Sigma power n fixes i, this implies sigma power 1, sigma 1 power n, sigma 2 power n, sigma k power n fixes i. We just argued in the right hand side of this slide that sigma 2 power n fixes i, it does not appear in i means, i doesn't appear in sigma 2 power n means it fixes i. Sigma k power n also fixes i, so we can conclude that only, so it fixes i, so sigma 1 power n fixes i, so sigma 1 power n must fix i, it cannot, see if it sends i to something else, because i is not present in sigma 2 and sigma k, you cannot send i back to itself under this product.

So sigma 1 power n fixes i. Similarly sigma 1 power n fixes every index appearing in sigma 1. So i was an index appearing sigma 1, if I was an index appear in sigma 1 , because sigma 2 power n, sigma 3 power n, and sigma k power n, they all fix , we can be sure that sigma 1 power n also fixes i. Because if doe not fix i the product cannot fix i, that is the point, because if i goes to j, how will j come back to i, under the product is suppose to come back to i, under the product of sigma 1 power n and sigma 2 power n , sigma k power n , i goes to i, so if i goes to j under sigma 1 power n j must come back to i, but it cannot, because if i doesn't appear in these indices, j also wont appear in these indices.

So i must go to i under sigma1 power n, similarly everything that appears in sigma 1 must be fixed by sigma1, this is to say, sigma 1 power n is identity. So sigma 1 power n must fix everything that is in sigma 1, of course it fixes everything that is not in sigma 1. Because sigma 1 fixes everything that is not in sigma 1, so sigma 1 power n is identity. It fixes every index,

(Refer Slide Time: 12:16)

but then order of sigma 1 is m1, and sigma 1 power n is identity. These two together imply that m1 divides n. This is also an exercise I have done in the previous videos, if order of an element is m but some other power of that element is e, then order must divide n. We have argued with sigma 1, we can argue with sigma 2, the same argument will show that, sigma 2 power n is also identity.

There is nothing special about sigma 1, sigma 1 power n is identity means sigma 2 power n is also identity. So m2 divides n , and so on, order of sigma k is mk and sigma k power n is also identity. By the same argument mk divides, so each mi divides n. Since each mi divides n, for all i , we have the lcm divides n. See if each mi divides n , n is a multiple, n is a common multiple of mi, but capital M is the least common multiple, and the property of least common multiple says that, least common multiple divides all multiples.

And in fact definitely we have, even if you don't agree this or you are not familiar with this it is the least common multiple, M is the least common multiple and n is a multiple, so we must have this, M is the least, we only need this for the moment, capital M is the least common multiple, n is a multiple, so M is less than or equal to n. So what we have shown is that now coming back to our sigma, sigma power M is identity and if sigma power n is identity for a positive integer, then m is less than n. So together these two facts imply that order of sigma is M. So this proves the proposition.

(Refer Slide Time: 15:07)

What we have shown is that if you have a product of disjoint cycles then order is the common multiple of the sizes, least common multiple of the orders of each individuals disjoint cycle.

So for example if you take the element we started with in the video (1 3 2 4) (5 6) (7 8) . So this has order 4, order 2, order 2. So what is the order of sigma? Recall that these are disjoint cycles which is important, so order is lcm of 4, 2, 2 which is 4. So order of sigma is 4.

So as I said it is important that the cycles have disjoint decomposition, the cycles are disjoint. Let us look at another example, let us take sigma to be (12)(123), these are not disjoint cycles. What is the order of this? In order to find that let us multiply it out. Where does this go? This we have done before, 1 goes to 2 , 2 goes to 1, so 1 is sent to itself, 2 goes to 3, and 3 goes to 1 and 1 goes to 2, so this is (2 3).

So sigma is a 2-cycle, but it is a product of, it is also a product of a 2-cycle and a 3-cycle. Sigma is a 2-cycle but it is also product of a 2-cycle (1 2) and 3-cycle (1 2 3). If the proposition applied to any product, order of sigma, actually it is two, because it is a 2-cycle. And we have already proved in a previous proposition that k cycle has order k, so order of sigma of 2, but lcm of 2 and 3 is 6. 6 is different from 2, so the proposition requires that the cycles are here.

(Refer Slide Time: 17:47)

The proposition does not apply, because (1 2) and (1 2 3) are not disjoint cycles, so to find the order of a permutation we have to find its disjoint cycle decomposition, if you have some cycle decomposition, you cannot say order is lcm of the individual orders. So only if you have disjoint cycle decomposition you have the property that order is the lcm of orders.

So I am going to stop the video at this point. In this video we have looked at cycle notation for elements of symmetric group, we have seen that every element of symmetric group has a decomposition into disjoint product of cycles or a product of disjoint cycles, we have seen that order of a k-cycle is k and we have seen that if a permutation has a decomposition into disjoint cycles, order of the permutation is lcm of the individual orders.

In the next video we are going to further study the cycle decomposition. Thank you.

Online Editing and Post Production

Karthick
Ravichandaran
Mohanarangan
Sribalaji
Komathi
Vignesh
Mahesh kumar

Web Studio Team

Anitha
Bharathi
Catherine
Clifford
Deepthi
Dhivya
Divya
Gayathri
Gokulsekar
Halid
Hemavathy
Jagadeeshwaran
Jayanthi
Kamala
Lakshimipriya
Libin
Madhu
Maria Neeta
Mohana

Mohana Sundari
Muralikrishnan
Nivetha
Parkavi
Poonkuzhale
Poornika
Premkumar
Ragavi
Raja
Renuka
Saravanan
Sathya
Shirley
Sorna
Subash
Suriyaprakash
Vinothini

Executive Producer

Kannan Krishnamurty

NPTEL Co-ordinates

Prof. Andrew Thangaraj

Prof. Prathap Haridoss

IIT Madras Production

Funded by
Department of Higher Education
Ministry of Human Resource Development
Government of India
www.mptel.ac.in