NPTEL

NPTEL ONLINE COURSE

Introduction to Abstract Group Theory

Module 05

Lecture 27 –"Symmetric groups II"

PROF. KRISHNA HANUMANTHU

CHENNAI MATHEMATICAL INSTITUTE

I will do, hopefully the proof is clear, and I will do just couple of more examples.

(Refer Slide Time: 00:21)

You take S5, so let us use this inefficient, but clear description of an element, let us say sigma is, 1 goes to 2, 2 goes to 3, 3 goes to 4, 4 goes to 5, 5 goes to 1. So what is the cycle decomposition? So this is called cycle decomposition.

So as I said, start with 1, 1 goes to 2, 2 goes to 3, 3 goes to 4, 4 goes to 5, 5 goes to 1, so sigma is a 5-cycle, so that is all, because you have exhausted all the indices, there is no further cycle, in general you will have a product of several cycles. In this example sigma was an element of S9, it is a product of 3 disjoint cycles. See when I say product I mean I have told you how to apply product of cycles earlier.

In this case, we start with 7 and see where it goes? It goes to 8. Because it is disjoint thing 8 will not appear again, so 7 goes to 8, 8 goes to 7, 5 goes to 6, 6 goes to 5, 4 goes to 1, 1 goes to 3, 3 goes to 2, and 9 is not represented here, because 9 goes to 9 itself. In this example, sigma is a 5-cycle, one more example, so let us take.

(Refer Slide Time: 1:57)

Let us take S5 again, let us take tau to be 1 goes to 1, 2 goes to 2, 3 goes to 4, 4 goes to 3, and 5 goes to 5. So what is the cycle decomposition of tau? So this is called tau. Tau is this, so you start with1, 1 goes to 1, so you have, that is just a 1-cycle. 2 goes to 2 again it is a 1-cycle, 3, now you start with 3, which is an index not covered yet. 3 goes to 4 and 4 goes to 3. So you close the bracket and finally 5 goes to 5. So this is stopped.

But remember our convention, we don't write, because 1-cycle is unnecessary to write, there is so information you gain by writing 1, 2 and 5. So, see tau is just a 2-cycle. In this case tau is a 2-cycle. So now the general proposition is every element can be written like this. Every element has decomposition as a product of disjoint cycles. Another property of this, of disjoint cycles, which is also clear, another property of disjoint cycles is that if, sigma and tau are disjoint cycles, then sigma tau equals tau sigma, that is in words, sigma and tau commute with each other.

(Refer Slide Time: 04:00)

See, remember that in general symmetric group is not abelian, S3, we have seen in example detailed description of S3 earlier, and we know that S3 is not commutative , so in general two elements of S3 do not commute with each other. For example, so recall, in fact

SN is not abelian, if n is greater than or equal to 3. So this is an exercise in fact. S3 and S4, S5 they are not abelian they cannot be abelian, S1 and S2 are obviously abelian, because S1 is just a group with one element, S2 is a group with 2 elements, any group of order 5 or less we saw is abelian. So those are abelian and in fact without that exercise it is clear that a group of 1 and orders in that exercise also it was very easy to conclude that group of order 1 or 2 is abelian.

But SN is not abelian, for example if you take (1,2) and (1,2,3). What is this? If this is sigma and this is tau, so remember how do we multiply, we start on the right side cycle, 1 goes to 2 and 2 goes to1. So 1 goes to 1 in this product, 2 goes to 3, and 3 goes to 3 under that, so 2 goes to 3, 3 goes to 1 and 1 goes to 2. So we close the bracket and again we don't write 1 cycle, so this (2,3). On the other hand, what is tau sigma? (1 2) 3, (1 2). So in this case 1 goes to 2 and 2 goes to 3, so 1 goes to 3. And 3 goes to 3 in this but 3 goes to 1 in this. So you stop there, 2 goes to 1, 1 goes to a2. So again we don't write the 1 cycle 2 consisting of 2 so we have (2, 3) and (1,3) and these are different.

These are different, so ((1 2)) times (12 3) is not same as ((1 2) 3) times ((1 2)). So in general SN is not abelian, however what did I say here?

If they are disjoint cycles, they commute with each other. In this case they are not disjoint cycles, ((1 2)) and (123) are not disjoint. Because the index 1 appears in both the index 2 appears in both, so they are not disjoint cycles, however if they have the same, if they do not have any common indices, we must have that they commute with each other.

So now let me prove that, if sigma and tau are disjoint cycles, so however so in general they don't commute with each other, but if they are disjoint cycles, then sigma tau is tau sigma. So why is this?

If you think about it, it is clear, because when you try to write the product, what do we do? We first look at indices that are in sigma, and you see where it goes, but we first see indices in tau and see where it goes. Wherever it goes it won't appear in sigma again, unlike in this example in this case 1 goes to 2, but 2 goes to 1, because 2 appears here, but if there is no index that is common to both sigma and tau, whatever happens in sigma stays within sigma.

So when we consider, the product sigma tau we look at indices in tau first. Because they are not present in sigma, because they are disjoint cycles, this is very important, because they are not present in sigma, it does not matter whether we consider their images, we consider them first or after sigma. This is just something that hopefully is very clear trying to write it, it may be necessary, but let us just illustrate this.

(Refer Slide Time: 09:13)

For example if you have (1 2) and (3 4) , this is sigma and this is tau. If you have (1 2) and (3 4), what I am trying to indicate here is, so look at the indices in tau, 3 is the first index, 3 goes to 4 but 4 is not present in (1 2). So 3 goes to 4 under the product also, similarly 4 goes to 3 under tau and 3 is not present in this. So 3 goes 4 , 4 goes to 3. Similarly 1 goes to 2 under sigma and it is not affected by what happens in tau so 1 goes to 2 and 2 goes to 1, so we might as well write this as, which is tau sigma.

If the indices are disjoint they are unrelated they don't interfere with each other, so we have no problem and we can just multiply them in any order, so the cycle decomposition, this means in the cycle decomposition of a sigma, I have already told you that every element has a cycle decomposition. Now I am telling you that in the cycle decomposition of an element sigma the cycles can appear in any order.

In the example above, in SN remember SN, we discovered that it is (1, 3, 2, 4), times (5 6) times (7 8). But now I am saying that there is no problem if we write it like this. (5 6) (1, 3, 2, 4) (7 8) or (7 8) (5 6)(1, 3, 2, 4), (7 8) (1, 3, 2, 4) (5 6), they are all same. That is because the indices are different, are disjoint, so whatever happens within (1, 3, 2, 4) , does not interfere with what happens with (5 6). And with what happens with (7 8). So I can blue in the order.

So the two important properties of cycle decomposition hat we have learned so far is, every element of SN has a cycle decomposition is, and the order in which cycle decomposition we write element is irrelevant. So order in which we write is not important, we can write it in any order. So some other properties of cycle decompositions.

(Refer Slide Time: 11:35)

So consider a k-cycle, use SN, let sigma be a k-cycle in SN, so we can write, sigma as, remember sigma can be written as (i1, i2, …, ik). So I must stress here that not every element is a k-cycle by itself, for example this element of S9, is not a cycle, it is a product of 3 cycles. So a cycle is just one cycle, so its cycle decomposition is itself, those are very special elements in SN. Sigma is a k-cycle means it is a single cycle, but in general elements of SN can be products of more than 1 cycles, in this example sigma is a product of 3 disjoint cycles.

Now I am considering a single k-cycle, I want prove the proposition that the order of sigma, in other words, order of a k-cycle is k. So recall what is an order of an element? In general order of sigma would be by definition the smallest positive integer d, such that sigma power d is identity element.

So we want to show that sigma power k is identity, and sigma power any smaller thing is not identity. So in order to do, that let us find out what are the powers of sigma. So sigma is 9i1, i2 up to ik). And recall what the meaning of this is? It sends i1 to i2, i2 to i3, so on finally i(k-1) to ik. And what happens to an index that is not inside i1 to ik, nothing happens, it is fixed by sigma. If a j is different to i1, i2, to ik it sends j to j, so we don't need to worry about it, j goes to j for any j that is different from i1 to ik.

So now what happens to sigma square, what is sigma square? Remember sigma square, because the operation in the symmetric group is the composition, is sigma composed with sigma. Where does i1 go under this, so i1 goes to i2 under sigma under another sigma it goes to i3. So i1 goes to i3 under sigma square, so I am going to keep track of the cycle of i1 under sigma , so i1 goes to i3 so I write it like this so (i1, i3. i1 next to is i3.

What happens to i3, let us figure out what happens to i3? Under sigma i3 goes to i4, and what happens to i4 under sigma it goes to i5, so i3 goes to i5. Similarly i5 goes to i6 then i7, i 5 goes to i6 under sigma and under another application of sigma i6 goes to i7.

So i5 goes to i7. So it keeps on going like this, which element goes to i1? So of course here I should write ik goes to i1, under sigma i(k-1) goes to ik under sigma, ik goes to i1 under sigma, so you have i(k-1) here. i(k -1) goes to i1. What happens to ik it must appear in the previous place somewhere in the middle.

(Refer Slide Time: 16:07)

So what we have concluded is sigma square is another, k-cycle. Remember sigma square is an element of the symmetric group. So it has a cycle decomposition, in fact it is a k-cycle itself. Because where is ik appearing here? See i(k-2) goes to i(k-1) under sigma under again sigma it will go to ik. So ik will appear here. So every element i2 will also appear, i2 will go, where does i2 go? ik goes to i1 and i1 goes to i2, so ik goes to i2. So they all appear here.

For example if I take sigma to the (1 2) (5 7), it is inside S7. What is sigma square? Sigma square is it starts with 1 and I just skip one step, so 1 to 2 and then 5, so it is (1 5). 5 goes to 7 under sigma so 7 goes to 1 so this (1 2 5 7), so 1 goes to 2 2 goes to 5, and 5 goes to 7, and 7 goes to 1, so 5 actually goes to 1.

2 goes to 5 and 5 goes to 7. So 2 goes to 7, so 7 goes to 1 and 1 goes to 2, so actually you can see in this example what I wrote here is just wrong. So sigma squared is not in general a k-cycle, as this example shows.

I should have not written that, so sigma squared is not in general a k-cycle, because may be not all indices are covered there, as this example shows, so sigma is a 4-cycle, but sigma squared is a product of two 2-cycles. Sigma is (12 5 7), sigma square it is (1 5)

(2 7). But doesn't matter, so sigma squared sends in any case, sigma squared sends i1 to i3.

What happens to sigma cubed? So I am going to keep track of what happens to i1 under each successive power of sigma, sigma sends i1 to i2, this is the first step, sigma squared sends i1 to i3, sigma cubed sends i1 to i4, remember the fact that we are saying sigma is a k-cycle, implicitly means that if it is a k-cycle, it means that i1, i2 and ik are distinct indices.

(Refer Slide Time: 19:39)

Otherwise there will not be k of them so I won't call it a k-cycle, and more than that, in a cycle we are not allowed to repeat elements , this is not a cycle ,because if 2 goes to 2, but 2 also goes to 1 under this, in a cycle we cannot have a reputation of an index, so if it is a k-cycle they are all distinct indices.

So now let us come back to this, sigma sends i1 to i2, sigma squared sends i1 to i3, sigma cubed sends i1 to i4. And you can see that sigma k-1 sends i1 to 3 goes to 4, 2 goes to 3, so this goes to ik. And this is not surprising, so I have to repeat k-1 times we apply this, i1 will go to the last index.

So since i2, i3 up to ik are all distinct from i1, remember that that is the point of being a k-cycle, this is not i1, this is not i1, this is not i1, this is not i1, they are all not distinct. Because (i1, i2, i3 .. ik) is a k-cycle, and sigma can't be identity, because sigma sends i1 to i2 which is different from i1, so sigma cannot be identity. I don't care about what it does to other elements, it is a i1 to i2, so identity element is supposed to send i1 to i1, but sigma sends i1 to i2, so sigma cannot be e.

Sigma square sends i1 to i3 so it cannot also be e. Because i3 is different from i1. So identity element sends i1 to i1, similarly sigma cubed can't be e and finally sigma k-1 cannot be e. So sigma is not e , sigma squared is not e, sigma cubed is not e, sigma k-1 is not e. So order of k, order of sigma, has to be at least k. So remember order of sigma is the least positive integer d, such that sigma power d is identity.

So here sigma is not identity sigma squared is not identity, sigma k-1 is not identity. So the order has to be al least k. Is it k? Let us find out what sigma k does. Under sigma k, i1 goes to i1, because under sigma k-1, i1 goes to ik, if you apply sigma again, it goes to i1. So far so good, sigma k has the chance to become be the identity element, because i1 goes to i1.

(Refer Slide Time: 23:12)

What about sigma k i2, so i2 remember, under sigma goes i3, under again sigma it goes to i4 and if you keep applying this, at some point you will get ik and then i1, then i2. So if you do k times, so sigma k of i2 also i2. Because it is the same, it is a cycle, and as I said cycle can start with any of the indices in it, so the I said here with i1 but (i1, i2, ik) can be written as (i2, i3, ik-1, ik, i1). And now i2 is the first one, in the previous calculation they also said the first one after k times we will reach the first one again.

So i2 after applying k times, we get to i2 again, so similarly, sigma k power i, any of them , so sigma is i3, sigma k power i4 is i4, and so on and finally sigma k power ik is ik. So we have sigma k is the identity element, right, because sigma k times i1 to i1, i2 to i2, i3 to i3, ik to ik but does it another indices which are not inside i1 through ik to themselves? Of course it does, because sigma itself sends any index that is not equal to i1, i2, …, ik to itself , so j is not in i1 up to ik, sigma of j is j, so sigma k of course will also send j to j, so in other words sigma k sends any index to itself. So sigma k is identity and sigma any smaller power cannot be identity, so this proves the proposition.

So sigma which is a k-cycle has order k, and so order of a k-cycle is k.

(Refer Slide Time: 25:44)

So for example the order of (1 2 3 5) is 4 because it is a 4-cycle. And it is a good exercise for you to check that in fact it is 4 by multiplying it out. So maybe I will just do quickly (1 2 3 5) squared, is 1 3, 3 goes to 1, so that is (1 3) . And 2 goes to 3 and 3 goes to 5 so (2 5). What is (1 2 3 5) cubed? So 1 goes to 5 and 5 goes to 3, and 3 goes to 2 and (1 2 3 5) to the 4th is identity. So this I will let you check, so check this, and of course the point of previous proposition is that you don't have to do this calculation every time. (1 2 3 5) you can immediately say, because it is a 4-cycle, it has order 4.

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

HYPERLINK "http://www.mptel.ac.in"www.mptel.ac.in