NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract
Group Theory
MODULE – 02
Lecture – 09 - "Types of Groups"
PROF. KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

Okay, so another important notion is that of a, so let G be a group and let A be in G, let's take an element of it, so I want to define the subgroup generated by A is the subgroup, so the subgroup generated by A so that is the term I'm defining here is this set, so this if you split out it looks like this, it has E, it has A, it has A squared, it has A cubed, it has this, it has also A inverse, it has A – 1 squared which is under notation A – 2, A -3 like this, okay, so this is denoted by let's say this symbol, the subgroup generated by, definition of this is this, so the subgroup generated by A is denoted by A within these brackets.

First of all, why, this is certainly a subgroup. This is a subgroup that I am trying to define a subgroup generated by A, why is this a subgroup? So it's very clear right, because identity is there, if you multiply two things here it is A power N times A power M so it is, as I commented in earlier video when I was looking at an example, you can take usual exponential rules, so if you multiply two powers of A, you get another power of A, and inverses are also there because A inverse is there, A squared inverse is A -2 and so on, so this is subgroup.

Not only that. If a subgroup H of G contains A then A power M is in H for every integer, right, because if H contains A and H is a subgroup, the properties of a subgroup say that A inverse is in H, A squared is in H, E is in H, so A power 0 is in H, A power -2 is in H and so on, so all powers of A are in H, in other words H contains the subgroup generated by, all this is supposed to imply, and all this implies that the subgroup generated by A is the smallest subgroup of G containing A. Nothing smaller than this can contain A, because once it contains A, the group properties guarantee that, if a subgroup contains A it must contain all of these elements, okay, so it's important to, this is an important notion, so subgroup generated by an element.

Okay, so now a very important definition here about groups. A group G is called cyclic, it's a cyclic group if there exists an element A in G such that the subgroup generated by A is G, okay, so in other words, G must be all powers of A, so if G consists only of powers of a specific element then we say that G is cyclic, okay, so this is an important class of groups. For example, Z under addition is cyclic. It is cyclic because, what is a subgroup generated by, by what, so namely this, what is this? This is equal to Z, because you take 0, you take all multiples of 1, so you take 1, 2, 3 times 1, 4 times 1, you take 0, you take negative of 1, you take twice the negative of 1, thrice the negative of 1, four times the negative of 1, this is equal to the subgroup generated by 1, but of course this is Z also, so Z is cyclic and it is generated by 1, so if G is a cyclic group there is an element A such that the subgroup generated by A is G, so in this case we say that G is generated by A or A is a generator of G.

In our example, 1 is a generator of G. In fact, -1 is a generator of Z also, 1 is a generator of Z as I explained here, but -1 is also generator of Z, because -1 multiples also cover all of Z. Is 2 a generator of Z? Is 2 a generator of Z? To answer this question consider the subgroup generated by 2, this is all multiples of 2, right, in the general notation I called it all powers of 2, but here the addition is the operation so it's all multiples of 2. And we have a name for this, it is 2Z, but this is not equal to Z, so 2 is not a generator of Z. In fact no number other than 1 and -1 is a generator of Z, okay.

So now some more notation here, so let us now go back to a general situation. Let G be a group and let A be an element of it. I want to define the order of A is the order of the subgroup generated by this, if this is finite, okay, order of an element A is the order of the subgroup generated by that element, if the subgroup is finite, otherwise if the subgroup is infinite we say that, we say that, the order of A is infinite, order of A is denoted by, we denote this by order ord (A), so order of A recall again is it is, it is obtained by looking at the subgroup generated by A, if it is a finite subgroup, if it's a finite group we say the number of elements of that is order of A, otherwise if the subgroup generated by is not finite, then order of A is infinite.

Okay, so as an example G is any group, order of the identity element is always 1, that's clear right because what is the subgroup generated by E, is just E, only things it contains are powers of E which is just E, so order of E is, so order of the identity element is always 1. On the other hand if you take the integers, what is order of A? If A is not 0 this is infinity if A is not 0, because for any nonzero element, so this is not, if A is nonzero, if A is 0 order is 1, if A is nonzero order is infinity because the subgroup generated by that is going to be infinite, because it is AZ it has infinitely many elements.

So now I want to do this with important example, and you are required to remember from an earlier video what S3 is so remember S3 is, recall S3 was the group, bijections, group of bijections of a 3 element set which we denoted by 1, 2, 3, and in the video when I discussed this in detail I used the notation F1, F2, F3, F4, F5, and F6 to denote all the bijections, so I would like you to compute orders of elements of, okay, and answer the question: is S3 cyclic? Okay, so I won't do that details and I will let you do the work, you can stop the video here and do the work and, no, no I don't mean you can pause the video here and do the calculations but I'll give you the answer in case for you to check, so if you remember the notation of this F1 to F3 from F1 to F6 from the one of the earliest videos, so you can remember that F1 was the identity bijection, so order of F1 is F1 is 1. Order of F2, and order of F3, and order of F4 will all be 2, okay.

So for example if you do the calculation you will see that the subgroup generated by F2 is just F1 and F2, because F2 squared is just F1. F2, F3, F4 were permuting 2 of the 3 numbers, and third one is kept fixed, so F2 fixed 3 and sent 1 to 2, 2 to 1, so F2 squared will be identity, so the subgroup generated by F2 is just {F1, F2}, so order of F2 is 2, so this is similar to, the same is true for F3 and F4.

On the other hand if you look at F5 and F6, the subgroup generated by F5 is actually {F1, F5 and F6}, I also asked you in an earlier video to completely describe the multiplication table of this, and if you did that it would be clear to you that subgroup generated by this is this, so ord and which is also same as subgroup generated by F6. so order F5 and ord F6, so you have 3 elements, you have 1 element of order 1, 3 elements of order 2, and 2 elements of order 2, so S3 has one element of order 1, always every group has one element of order 1, 3 elements of order 2, and 2 elements of order 3.

Now the question that I asked earlier: is S3 cyclic? Okay, so remember from an earlier slide, what is a cyclic group? So somewhere I missed this, yeah, so a subgroup, a group is cyclic if there exists an element A in G such that A is the generator of G. So now is S3 cyclic? We have 3 possible elements, do they generate S3? Does F1 generate S3? Certainly not because F1 is identity, does F2 generate S3? No, because F2 the subgroup generated by F2 is just {F1, F2}. Does F3 generate S3? No, again order is 2, so similarly F4 does not generate S3, but neither do F5 and F6, so because the subgroup generated by F5 is simply 3 elements, not all of S3, similarly subgroup generated by F6 is 3 elements, so S3 is not cyclic, that is a point.

So as this example shows I'll give this as an exercise and I will let you work this out in detail, it's a good exercise to understand the concepts. A group, let's say a finite group, let G be a finite group, let's say, of order N. So it has N elements, then G is cyclic if only if G contains an element of order N, because remember G is cyclic means G must be equal to the, equal to a subgroup generated by some element, G has N elements, so if G is cyclic G must contain a sub element, subgroup generated by which has N elements, so that element is order N. If G contains an element of order N then the subgroup generated by that element will be of order N, but G already has N elements so the subgroup also has N elements, so G must be equal to that, okay so the proof I just said orally you should combine all the details I said and conclude that, a finite group is cyclic if it is only if it has an element whose order is equal to the order of the group.

Okay, so also another exercise for you, and this one I will quickly workout. Suppose that G contains no subgroups different from {E} and G, so note that every group as I remarked earlier, every group contains 2 obvious subgroups, namely the trivial subgroup and the full subgroup, suppose that some group G does not contain any other subgroup, okay, then G is cyclic.

Why is this? So I'll write the solution for this, okay, so suppose we take an element, okay, so actually if G is actually all of E, G is a single element group, then it is cyclic, right because this is certainly cyclic. So assume that G is different from {E}, so that means G contains some element different from E, so let say A is in G, A different from E. Now consider the subgroup generated by A which is, which we denote by this symbol, so it cannot be equal to this, right, because A is not equal to E and the subgroup generated by A certainly contains A so it's not equal to {E}.

Now what is the hypothesis on the group G? It says that G contains no subgroups different from {E} and G, right, this is a subgroup, A the subgroup generated by A is a subgroup, it is different from {E}, so it must be equal to G, right, because G contains subgroups, no subgroups other than the trivial subgroup and the full group and we have constructed the subgroup which is different from trivial subgroup, it must equal all of E, so G is cyclic by definition, right, as soon as you have an element whose subgroup generated by which is equal to G, G is a cyclic, so that completes the solution.

Okay, so I will now give you some important subgroups for any group, so now let G be any group, okay, so I am going to define a few subgroups which are very important and we will study them later. The first one is the center of G denoted Z(G), it is all elements, let's say g in G which have the property that Ag = gA for every, okay, so you need to stare at this for a minute to understand this carefully. Center of G denoted by this symbol is the collection of elements of the group which commute with everything else, so Ag must be equal to gA for every small A in G, okay, so the proposition is that Z(G) is a subgroup, so let me prove this.

The previous slide contains the definition of Z(G), what is a subgroup? We must show that it is closed under the operation of G, so let's say G1 and G2 are in Z(G) to prove, we want to prove G1G2 is in Z(G), right, we want to prove this, what does this mean? In order to be in Z(G) it must commute with an arbitrary given element of G, so let's take an arbitrary element of G and see what happens to G1G2 times A, this by associativity of the group is G1G2 of A, right I can put the bracket here, but G2 remember is in the center, so G2 commutes with A, so this is G1 of times AG2, but again applying the associativity this is G1A times G2.

Now I'll continue here. G1 is in the center, let's use that now, so it is AG1 G2, again using associativity it is AG1 G2, so now we are done because G1 G2 times A is A times G1 G2, so that tells me that G1G2 is in Z(G), so Z(G) is closed, is the identity element in Z(G)? It is certainly there because E times A is A times E = A for A and G, so certainly the identity element always commutes with everything so that is okay, and finally if G is in Z(G), is G inverse in Z(G), let's check, so we want to check G inverse times A must be equal to A times G inverse, so what is this? So this is, if you do, so I claim that this is equal to A inverse G inverse, so if you recall I gave an exercise or I mentioned this in an earlier video, in any group AB inverse is B inverse A inverse, so this is, I'm applying that here, so basically applying this, G inverse A is the inverse of, I have to interchange the letters here, so it's A times, inverse of A times G the whole inverse, okay, so this is correct, right.

But G is a element in the center, so G commutes with everything, so this is G times A inverse, nothing I only interchanged within the bracket I interchanged these two, but now again applying this, this is GA inverse whole inverse is A times G inverse, okay, so G inverse is in Z(G), so hence Z(G) is a subgroup, this completes the proof. So the center is a subgroup consisting of all elements that commute with everything. So as an easy exercise for you if G is abelian then what is the center? Center is the set of elements that commute with everything, so certainly it must be everything, okay, so this is not surprising.

One final thing I'll define in this video and we will stop after that. So let G be a group and let A be an arbitrary element, the centralizer, so this is the definition, centralizer of A, denoted C(A), is C(A) is all elements of the group which commute with A, okay, so earlier when I defined the center, it is elements of G that commute with everything, AG = GA for every A in G, now I don't care about everything, I fixed A and I only define it to be all things that commute with that specific element, so as before and this I'll leave for you as an exercise and prove it maybe in the next video, C(A) is a subgroup of G, the center is always contained in C(A) for all A in G, okay, and also if G is abelian it is clear that C(A) is equal to G for all A in G, okay, so these are three exercises for you and I'll maybe comment on some of these in the next video, so I'll stop now, in this video, we've looked at definition of a subgroup, we've looked at various examples of subgroups, we have shown that all subgroups of Z are obtained as multiples of a fixed integer, we've looked at subgroups generated by an element and defined the order of element, cyclic groups and finally we have defined center of a group and centralizer of an element of a group.

Online Editing and Post Production

Karthik

Ravichandran

Mohanarangan

Sribalaji

Komathi

Vignesh

Mahesh Kumar

Web Studio Team

Anitha

Bharathi

Catherine

Clifford

Deepthi

Dhivya

Divya

Gayathri

Gokulsekar

Halid

Hemavathy

Jagadeeshwaran

Jayanthi

Kamala

Lakshmipriya

Libin

Madhu

Maria Neeta

Mohana

Muralikrishnan

Nivetha

Parkavi

Poonkuzhale

Poornika

Premkumar

Ragavi

Raja

Renuka

Saravanan

Sathya

Shirley

Sorna

Subash

Suriyaprakash

Vinothini

Executive Producer

Kannan Krishnamurthy

NPTEL CO-ordinators

Prof. Andrew Thangaraj

Prof. Prathap Haridoss

IIT Madras Production

Funded by

Department of Higher Education

Ministry of Human Resources Development

Government of India