NPTEL

NPTEL ONLINE COURSE

Introduction to Abstract

Group Theory

MODULE – 01

Lecture – 04- "Basic properties of groups and

Multiplication tables"

PROF.KRISHNA HANUMANTHU

CHENNAI MATHEMATICAL INSTITUTE

So far we have in the previous videos we have studied several examples of groups and we formally saw the definition of a group, so let's continue this, we will study in this video some properties of groups and some important types of groups, okay. So let's recall, I'll spend 2 minutes of recalling, so if G is a group remember in the other video I said G is a group under a specific operation, so let's say under an operation star, so that means it is closed under the star, in other words G x G to G there is a binary operation, there exists an identity element, every element has an inverse, and finally star is associative. The important examples that we have looked at, I will not explain everything but ,Z, R, Q, C under addition Q star which is non-zero rational numbers, R star which is nonzero reals, and nonzero complex numbers under multiplication, positive reals and positive rationals under multiplication, we also looked at SN bijections okay, and I think we looked at roots of, nth roots of 1, unity, we looked at rotational symmetries of an equilateral triangle, and we also looked at some matrix groups, so this is just to recall what we have done so far.

So next I want to study some examples some properties and different types of groups, so the first I want to, type I want to define is a group G, let's say star is called "abelian", it's also sometimes called a "commutative group", but we will

most of the time use the word abelian if a star b is equal to b star a for all a, b in G. So remember that a group is a set along with a binary operation and we say that it's abelian if it does not matter in which order we multiply or compose the any given two elements, so and if you recall when I first looked at some examples of groups and I looked at Z in particular, I noted that this property holds in Z, but I commented there that this is not a critical property for a group, so we don't ask for it and we just give a new name to groups which have that property, so obviously the examples will include Z, because the addition of integers is abelian, also similarly Q, R, C, Q star, R star, C star, Q positive reals, positive rationals, positive reals are all abelian, okay, because I am not emphasizing the operation here, because it's understood from the earlier videos, in Z, Q, R, C the operation is addition, it is abelian. Q star, R star, C star, Q+, R+ there are all multiplication, they're abelian, so this is easy, usual multiplication and addition of numbers is abelian, but not everything is abelian as we saw, SN is not abelian. We specifically saw that S3 was not abelian in the earlier video where we looked at S3 in specific detail and concluded that it's not abelian, so actually I should write for N at least 3, if you look at and I'll give this as an exercise. Remember SN is defined for any positive integer. So S1 and S2 are abelian, S1 is just a bijections of single element set, so S1 itself will be a single element group, S2 is a bijections of a two element set, so there will be two such bijections and it will be abelian, okay, so this is an important class of groups, they are called abelian groups if the group operation is commutative, meaning a star b is same as b star a, we also use the word, we mostly use the word abelian, okay.

And also we have another natural definition, a group G is called finite, if the number of elements, very natural definition, so G is a finite group if, it has finitely many elements, okay, so as you can see here I've already omitted to write the binary operation because it's not required for the definition, it's a purely set-theoretic notion, a group is finite if as a set it is finite. So again examples: SN is finite, okay, as an exercise you can do this, SN has, this is true for all N greater than or equal to 1, SN has N factorial elements, and of course Z, Q and so on the other list of groups, remember Z, Q, R, C, Q star, R star and so on are not finite groups, okay.

A related definition: if G is a finite group then the order of G is defined to be the number of elements of G, okay, it is denoted by this symbol, okay, so G with two vertical bars is by definition the order of G, so for example, order of SN, by the exercise I mentioned earlier is N factorial, okay, so we only usually talk about order for finite groups, because otherwise number of elements is infinite, okay.

So next, I want to talk about, so important distinction between groups is between finite groups and infinite groups, and we have examples of both kinds of groups in our earlier examples. So now some properties I want to discuss of groups, these are very general things, I will check some of them, leave the others for you to verify. One property that comes in very handy is called cancellation property. What do I mean by this? Okay, so let's say G is a group, okay, let's say I have 3 elements in it, so a, b, c are in G. Cancellation as what to the name suggest, so I can cancel elements in the following sense, so suppose that I have ab = ac, so here I'm writing a times b, or a star b really in general, but just for the sake of convenience of notation I don't put star, I really mean, but as you will agree it's easier to write without star so I'll just write ab = ac, but when I'm talking generally about a group I will suppress this star symbol so and I write ab= ac, okay, so then so I have ab, a star b, or a times b I use all this words, just its easiest to say ab = ac, so if ab = ac then the cancellation properties says we have b = c, so ab = ac gives b = c, in other words that is we can cancel a, so we are used to doing this in school, right, if we have ab = ac we can cancel, this is okay, this is what I'm doing, but in an abstract group this is a valid operation, this is what I want to now emphasize, why is this? So let's do this, first time you are doing, seeing this perhaps, so let's check this carefully step by step, so what are we given? We have given, we have been ab = ac, so I'm going to use in the proof now, only properties of groups that are contained in the definition, I do not want to use any properties of numbers or functions or rotations, any kind of complex numbers, anything that I know before I do not want to use, I only want to use group axioms or group properties, this is what the subject of abstract group theory does, so I have, this is an equation in G.

Now I can multiply, so again let me remind you I use the word multiply to simply mean, I apply the binary operation by a inverse, and a inverse also let me remind recall a inverse is the notation for inverse of a, so if you have two elements that are

equal in a group by multiplying by a inverse they will remain equal, okay, so if ab = ac, a inverse times ab = a inverse ac, that is just a set theoretic property, if you have two elements and you multiply by the same element they will remain equal, this is the meaning of binary operation. But now I'm going to use the associativity of my group operation, so this is using associativity, so I have used the property that we have associativity and I have earlier also used the property that I have inverses, so remember that, that's an axiom of a group. In order to even talk about an inverse I need to have it in the group, which exists because it's a group, similarly I have used associativity at this point, but now because a inverse is inverse of a, this is simply e times b, this is because a inverse a is identity, this is the definition of inverse, and what is the definition of identity? e times b = b, this is because e is the identity.

So in other words we have used all the properties, right, we have used associativity, that we have inverses, that we have identity element, and of course we have a binary operation has been used throughout, so please remember what I have just, I wanted to prove, so you have ab = ac implies b = c. This should recall for you something that you have done in school or for a long time, when you are solving this should remind you, solving linear equations, okay, so you have 2X + 3 = 5X + 9 something like this, so here if you want to do this, if you solve this what do you do? You can subtract 2X and subtract 9 so this will give you 3X = - 6 implies X = -2, so this we are used to doing in some sense without thinking a lot whether it is valid or not, it's not always valid, and in order to make it valid we have define proper mathematical structures, and a group does that, a group allows you a systematic correct setting where you can perform such operations, many of the things adding, subtracting, multiplying, cancelling, all these are valid operations in a group, so this is just a side remark, don't think too much about it, I'm just trying to justify why cancellation property is something that we are used to dealing with, and in the new setting of an abstract group we have it.

Once you have a cancellation property we can do some more things. So a group remember, a group always contains the identity element, I keep saying, in all my videos I've been saying that existence of the identity element is an important part

of definition of a group, but I've been sloppy if you noticed in earlier videos, whether sometimes I say it has an identity or the identity, but now I will justify everything by saying a group has a unique identity element, namely a group cannot admit two distinct identity elements, and hence we are allowed to say the identity element of a group, why is this? Why does it have a unique identity? So suppose not, so suppose so why? We have to prove this, right, anything we write we have to prove, so suppose that G has two identities, let's say e and e prime, you note that we have been using the letter e to denote identity element of a group, so e and e prime let's say serve as the identity, and at this point let's recall also the definition of the identity element, what is an identity element? It's an element which has the property that when you multiply any element of the group with it, you have to get the element back.

So for example when you multiply e with e you get e, this is the definition of the identity element, so e is the identity element, small e is some other element, I mean it's some element of the group, so e time e is e, but what is e times e prime? e prime is also the identity element, an identity element of the group, e is an element of the group so e times e prime must be e, because e prime is an identity element, this is because e prime is the identity element, e prime is the identity element means g times e prime is equal to g, for every g in the group G, I'm applying it to e, so e times e prime is e, but then e times e is also e, so e times e is equal to e times e prime, but now cancellation property says, remember this is exactly the setting of the cancellation property ee = ee prime that means e = e prime as we wanted, so if you start with two identities they are equal, so a group has exactly one identity, it must have one identity, it cannot have two different identities, also so this is one property that immediately follow from cancellation property.

Another property, any element of G has a unique inverse, okay, again if you go back and see the videos earlier, I've been sloppy sometime I say, let g be the inverse of g, let g inverse be the inverse of g or let it be a inverse of g, I've been, maybe inconsistent in my usage, but again I will prove that inverse has to be unique, so let say g is an element of, all the arguments here are very standard arguments, but they are critical arguments to understand group theory, how to

work with abstract groups, in order to understand and familiarize yourself with these things, you have to understand these arguments, they are simple but if you are seeing them for the first time they will require some getting used to, so let's say g is, a small g is an element of capital G, so suppose g has two inverses, say g1 and g2, remember my claim is that every element has a unique inverse, certainly it has some inverse because that's the definition of a group, every element has an inverse, but suppose it has two inverses, so then we now that g and g1 is equal to the identity element, by definition of an inverse, but so as g times g2 because g2 is also an inverse of g, but again cancellation property gives you, forget this, you apply cancellation property to this, it gives you g1 = g2, so again very simple, but you conclude that, cancellation property immediately gives you inverse has to be unique.

One more such thing I want to say, if you take, let's say g1, g2 are elements in a group, so suppose that g1g2 is e, then automatically g2g1 is e, okay, so remember that I'm working with an arbitrary group G, it's not necessarily abelian, I cannot in general switch, so note in general G is not abelian, so it is not true that g1 times g2 = g2 times g1 for two elements g1, g2 of G. It is certainly not true that g1g2 = g2g1 for two elements in a group in general. However, if g1g2 = e it must automatically mean that g2g1 = e, so in other words if g2 is inverse of g1 they commute, and this is again an easy application of the cancellation property. Let's try g1g2 = e, then, so then what do we do? So if you multiply by, so I want to conclude that g2 = e, g2g1 = e, let me now continue so g1g2 = e, so by multiplying both sides by g1 inverse, what do I get? g1 inverse, okay, so I don't need this, so I have this, so I'm just multiplying this equality by g1 inverse on both sides which I can do. Now apply the associativity, this is very similar to the work we have done in proving cancellation property so we have g1, remember g1 inverse e is equal to g1 inverse, because e is the identity element, this means because g1 inverse g1 is e, and finally this means g2 is g1 inverse, note that that means if g1 times g2 is equal to e using group axioms so we are able to conclude g2 is g1 inverse, and earlier in the previous slide I have shown that, inverse of an element is unique, so g2 is the unique inverse of g1, so that means now let's see what we want to prove, g2 times g1 to prove, the whole thing here is to prove if g1 g2 = e, then g2 g1 is also equal to e, so why is this true, but because we have already concluded g2 is g1 inverse,

so g2 g1 is g1 inverse g1, but g1 inverse g1 is, by definition of the inverse, identity, so if g1 g2 is identity, g2 g1 is equal to identity. In order to check something is the identity element it's enough to check the, something is the inverse, it's enough to check that product in one direction is identity.

And similarly one more property, maybe I'll leave these as exercises for you, very similar to the work that we have done in these things, so if g is an element of G, then g inverse whole inverse is g, so this is exercise one for you, this means that inverse of g inverse is g which is actually if you just write out what it means is obvious. Similarly if g and h are elements of a group G then the inverse of gh is h inverse times g inverse, so these are also easy exercises that I encourage you to do, just they will follow from the definition of inverses and group axioms, okay.

So and some more notation now I want to introduce in order to talk about multiplication tables, so if G is a group one can write down multiplication tables which are a compact way of describing the entire group, so and these make sense really only for finite groups, so let G be a finite group. Recall that a finite group is a group which has only finitely many elements. So for example S3 or group of, so a group of nth root of unity, these are all finite groups, so multiplication table as I said is a table which completely describes the group, so for example if you take the group of fourth roots of unity, if you recall from earlier today, earlier in the videos I defined these group, which is the group of fourth roots of unity, so every element in this group is a fourth root of unity, so here of course i is the square root of -1, so i is the complex

square root of -1, so if this group the multiplication table of, by multiplication table of this group, I mean the following, so I'm going to draw a table like this, I'll have one row for every element of the group, and similarly one row, one column for every element of the group, okay, so I'm going to draw a grid in some sense, so multiplication table, so clearly this only is possible, if the group has only finitely many elements, if it has infinitely many elements we cannot just contain the information in a table like this.

So in any position for example if this position, I have i in the row and -1 in the column I'll write down the product, so in this case it's –i, so for example let's just do one, one times anything is itself, so this is just this, -1 is -1, 1 – i and i, here I have i, i times -1 is –i, i times i is i squared which is -1, i times –i is –i squared which is 1, -i times 1 is –i, -i times -1 is i, -i times i is 1, -i times –i is -1, okay, so this is the multiplication table of this group of fourth roots of unity. And if you just stare at this table for a minute, and if you forget the first row and the first column only focus on the interior part of this table, so these are just labels, okay, forget those, each row of the table is just listing the elements of the group, no element can repeat here, and no element can miss from this list, for example the group is 1, -1, i, –i, here you have that in different orders you have listed all these elements.

Similarly each column contains all the group elements in some order, for example this column here i, – i, -1, 1 this is really a property of cancellation that's, you can do in a group, okay, so because you can cancel no two elements in any row or column can repeat themselves, okay. And as an exercise and this is again a very good exercise for you to familiarize yourself with calculations in a group, write down the, remember S3 from earlier video, S3 was the group of bijections of a 3 element set, so if you recall I have used this notation, okay, there were three such bijections if you go back to the beginning first video, I've completely described each element here F1 was the identity bijection, F2 is the bijection which fixes 1 and interchanges two elements, so I don't remember exactly what it is, but go back to it and write down the multiplication table, so along these lines that we have done for this group, it will have 6 rows and 6 columns and you have to fill in each, each spot in the table and as a way to check your answer, make sure that it, the table that you come up with that the end of the work has a property that this entire group is listed in each row and each column, if some element is repeated then you have a made a mistake, if some element is missing you have made a mistake, so make sure that you verify that each element appears in each row and each column exactly ones.

So I'll stop with this today, in this video please make sure that you do the exercise that I have assigned and when we meet next time we are going to study subgroups of a group and look at more properties of groups.