NPTEL

NPTEL ONLINE COURSE

Introduction to Abstract

Group Theory

MODULE – 01

Lecture – 05- "Problems 1"

PROF.KRISHNA HANUMANTHU

CHENNAI MATHEMATICAL INSTITUTE

Last videos we have looked at definition of a group, we looked at various examples, some basic properties of groups. So let me start today this video by working out some examples and exercises on groups, then we will study some more notions of groups, okay. So let start with a question, so I'll do a few exercises now and I'll work them out in detail so that you can do more similar examples.

So let's say I ask whether the following are groups, okay. So first let's say the underlying set is Z, we have seen in the previous videos that Z is a group under addition, but here I am giving a different binary operation, let's say I define, this is the definition, so I'll define a star b to be a – b, so certainly this is a binary operation because if I take two integers apply star which in this problem is just taking the difference you get an integer, for example if you do 5 – 3 you get 2, so similarly 3 – 5 is -2, so it is a binary operation, so far so good there is also an identity element, right, because 0 is the identity element, if you subtract 0 you get the element back, but actually I have to be careful, right, is this true really, is 0 the identity element? Certainly if you do a – 0, so a star 0 is a – 0 which is a, that is okay, but remember that we want 0 star a to be also a, but 0 star a is 0 – a which is – a, so actually 0 is not the identity element and you can check that, so 0 is not identity.

You can in fact check that there is no identity, that is because really 0 is the only possible identity because when you subtract 0 from a you get a, if you subtract anything else you don't get a, and you can also check that star is also not associative, okay, so I will simply write here, for example if you do 5 – (3 – 2), that is 5 – 1 that's 4, whereas (5 – 3) – 2 is 2 – 2 which is 0, okay, so it's not associative, so this is not a group, so this is not a group, okay, so this should suggest to you that operation is very important, right, subtraction is a very natural operation but under it the integers do not form a group.

Okay, let me look at a different example now, let's look at the same set, let's look at the same set but now I define a new operation, again the set is set of integers, but the operation is the following, so I do a star b is defined to be a + b + ab, okay, so this is again the definition of an operation, so for example if you do 3 star 5 you get 3 + 5 + 15, so that's 23, so this is certainly a binary operation, because if you perform this operation on integers you to get an integer, so this is a binary operation.

Is there an identity element? So if you do a star 0 you get a + 0 + 0 which is a, and if you do 0 star a you get 0 + a + 0 which is a, so this is true for all a in Z, so 0 is the identity element so that's good, so we have an identity element it's a closed operation. So is it associative? How do you check associativity? We want to do a star b star c what is this? This is, first I'm doing a star b so this is a + b + ab star c, this is, remember that when I, star I take the first one plus the second one plus the product of the two, so here the first element is a + b + ab, second element is c plus the product, so that is ac + bc + abc so that is the element a star b in bracket then star c.

On the other hand if you do a star (b star c) this is a star b + c + bc, okay, now again remember star means we take the sum of the two terms and then add the product of the two terms to this, first two terms so you get a + b + c + bc + the product which is ab + ac + abc, so now if you actually look at this two these are equal, because a is there, b is there, c is there, ab, ac, bc are there, abc is there, so

these are equal. And so star is actually associative also, okay, so it has three of the four properties that we want, but we need to check now for inverse, so what would be an inverse of this? So we want, and we have already noted that the identity element is 0, so we want, given an element a in integers, we want, what do we want? We want b which is another integer such that a star b is 0 because that's the definition of inverse, and remember that b star a is also a so that is okay, if b has this property it will automatically have this property.

Okay, but what is a star b, that means a + b + ab must be 0, okay, so we know a, we have to solve for b, so let's try to solve for b, so this will be a + b times (1 + a) = 0, so we can try to write it like this b times 1 + a = - a, so b should be – a divided by 1 + a, okay, this is what b should be if a star b is 0, but now there are problems here, first of all this is not an integer, if a is an integer this is not an integer, in general right because you are dividing by this, so for example if a is 2, b should be – 2 divided by 3, this is not in Z, so star does not have, does not admit inverses, okay, so (Z, star) is, we can immediately conclude that it is not a group.

Note that it has 3 properties, that's okay, binary operation identity associative, but it doesn't admit inverses so it's not a group, okay. But let's look at bit more closely at this operation, why

did inverses not exist here, because we have to consider rational numbers, so how about enlarging our set, so how about the same operation star but on let's say Q, the set of rational numbers? So here in the previous page we saw that the inverse of 2 under this operation should be – 2/3 which is not an integer but it is a rational number, so it looks like star must admit inverses in rational numbers, but remember what is the inverse of a? It should be, if you recall, it should be – a divided by a + 1, this is okay, it is in rational numbers but there is a problem, it is not defined when a is -1, because when a is -1 the denominator is 0 here, so this is not a well-defined number, so even if you take the larger set of rational numbers the star operation will not have inverse for -1, so it will have inverses for every other element, because 1 + a will not be 0, so – a divided by 1 + a is a well-defined rational number, so a = -1 is only problem.

So now we set, let's Q minus, okay, so in other words I'm removing – 1 from this set, so I am looking at the set of rational numbers, different from – 1, so let's say G is this, if G is this so I should not write, G is the collection of rational numbers different from – 1, then what we have verified says that G star is a group, recall that star is again as before it is a + b times a + ab, so under this G star is a group, if you eliminate – 1 from Q you can make it a group, okay, so this

example is a good example to keep in mind, because we started with Z under this operation, we started with Z under this operation we saw that it's a binary operation it has identity element, it is associative, however it doesn't have inverses in Z, so if you enlarge your set and consider all rational numbers then it has inverses except when we are looking at – 1, so we have removed it from the set, and we've only looked at rational numbers different from – 1, then G star is a group, okay. So sometimes we have to add more elements, sometimes we have to delete some elements in order to obtain a group.

Let's look at another example, so I don't recall the numbering here, so maybe this is the third example, so let's look at the set of rational numbers which have the property as I will write now, so rational numbers can always be written like this, okay, they are ratios of integers, so let's say a and b are co-prime, co-prime means they have no common factors, we say that a and b are co-prime, so I'm going to quickly define in case you are not familiar with this word, if they have no common factors, okay, so for example 6 and 10 are not co-prime, because 2 divides them. On the other hand 2 divides 6, 2 divides 5 so they have a common factor, on the other hand 6 and 9, actually 6 and 9 are also not co-prime, but if you take 6 and let's say 25, only factors of 25 are the 1, 5, and 25, factors of 6 are 1, 2, 3 and 6, so there is no common factor so these are co-prime.

When you write a rational number you can always cancel all the common factors so you can write it in the reduced form, so I take reduced form, so a, b are co-prime and suppose that 5 divides b, this is my set, so the set that I'm considering is set of rational numbers in the reduced form where the denominator is divisible by 5, so for example if you have 1/5 is in G, remember but 1/4 is not in G, remember that

you have to consider the reduced form, for example 1/5 is also same as 2/10, sorry so 1/4 is also same as 5/20, right, and you can look at this and say 5 divides 20, so 5/20 belongs to G that's not correct, I must first cancel all common factors and then ask whether 5 divides the denominator, okay, so 1/4 is not in G.

Is this a group, is G a group under addition of rational numbers? So I can add rational numbers in fact Q under addition is a group, I'm asking for a subset of that under the same operation is it a group, so what is the, so here you can check that various properties fail here, for example even the closure is not true, for example if you take 2/5 and 3/5 to it, remember 2/5 is in G, 3/5 is in G, 2/5 and 3/5 are in G because they are in the reduced form, and 5 divides the denominator, but what is 2/5 + 3/5 that is 5/5 which is not in reduced form, so you have to cancel and you get 1/1, it is now in the reduced form, but 1/1 is it in G? you have to ask yourself whether 5 divides the denominator, it does not, so 1/1 is not in G, so this is not a group because it's not even a binary operation, so it's not a group because G is not closed under addition, so this is not a group, so is this clear? So G, as defined here is not a group because it's not closed under addition.

Now let me modify this, let me take G prime, I use this G dash to denote a different set now, this is all rational numbers, again a and b are co-prime so the rational number is in reduced form, but unlike in the previous example now I demand that 5 does not divide, so by the way when I write this symbol I should have remembered when I write 5 this symbol, this means 5 divides b, so b is divisible by 5.

And now let say 5 does not divide b, so it is very similar to the previous example but it's very different also, because now I want the denominator to be not divisible by b, for example here 1/2 is in G prime, but 1/2, 1/5 is not in G prime, 5 does not divide 2, so 1/2 is in G prime, 5 divides 5 so 1/5 is not in G prime.

Is G prime a group under addition? So now the same question, the previous example also I asked is G prime a group under addition, is G a group under addition, and we saw that it doesn't even satisfy the first property, it's not a binary operation, addition is not a binary operation so I conclude that G here was not a group.

Now I have modified G, I've looked at G prime and now I'm asking is it a group under addition, so let's ask, let's take a/b and c/d are in G prime, so let them be in G prime, so in particular remember that they are in reduced form, and 5 does not divide b, 5 does not divide d, what is their sum? So if you sum them it is a/b + c/d and this is simply ad + bc divided by bd.

Now the question is, is this in G prime, we've started with 2 elements of G prime, we have taken their sum and seeing, asking whether the sum is in G prime, the previous example the sum is not in G, sum of two things in G is not in G, in this case, is it true?

Now the point is first of all this may not be in reduced form, but that doesn't matter because note that 5 does not divide, remember by definition 5 does not divide a, and 5 does not divide b also that is because, that is because a/b is in G prime, and a/b is in reduced form, so 5 does not divide b, c/d is also in G prime so by definition of G prime 5 does not divide d.

Now a property of prime numbers says that if 5 does not divide a, and 5 does not divide b, 5 does not, sorry, I should not write a here, remember 5 does not divide b is what I should write. 5 does not divide the denominator, 5 does not divide b, 5 does not divide d in the second example, so 5 does not divide bd, because one definition of prime number is that if 5 divides bd the product, then it must divide either b or d, so that's not the case, it does not divide b, does not divide d. So if 5 does not divide bd, now let's look at this, let's look at this rational number, while it may be the case that this is not in reduced form and you might have to cancel some factors, but 5 does not divide bd as it is already, so if you further cancel some factors there will be fewer factors, so 5 will definitely not divide that new factor, after cancelling whatever is the denominator 5 does not divide it also, so in the

reduced form after you find the reduced form of this you can conclude that this is in G prime.

So let me repeat the argument again, why I am saying that this is in G prime, because 5 does not divide b times d even after cancelling common factors of this ratio whatever is the new denominator also will have the property that 5 does not divide it, because in the new, after cancelling the new denominator will have fewer factors than bd, bd does not have 5 as a factor so after cancelling some whatever you get will continue to not have 5 as a factor, so this will be in G prime.

So in other words the upshot is that G prime is closed under addition which is the first property that we want for a group, so addition is a binary operation on G prime. So now let's verify the other properties, for example what is the identity element for addition? It must be 0, so you have to ask is 0 in G prime, it is, because 0 is 0/1 and 5 does not divide 1, so 0 is in G prime, this is okay.

What is the inverse of a/b? Inverse of a/b is - a/b, and if a/b is, if a/b is in G prime, then 5 does not divide b, right, that is the definition, it's in the reduced form and 5 does not divide the numerator, so then obviously – a/b will be also be in G prime because denominator is the same, 5 does not divide b, so inverses exist and addition is certainly associative, that is because addition is associative on the set of rational numbers, so this is okay, inverses exist it is closed under addition there is identity, so G prime is a group, we conclude that G prime is a group under addition. So again this example is very nice to keep in mind because we have, in earlier we have looked at G which is all rational numbers were 5 divides the denominator it's not a group, whereas if you modify the definitions slightly and say 5 does not divide b, it becomes a group, okay, so this is an important group that we will, it's an example of what we will later call a subgroup of a group, so we will come back to this later, but we will say that G prime is actually, I'll write it here just so that you keep in mind, I will refer to this later, G prime is a subgroup of Q, okay.

So this is as of now it may not mean anything to you, but we will keep, we will come back to this.