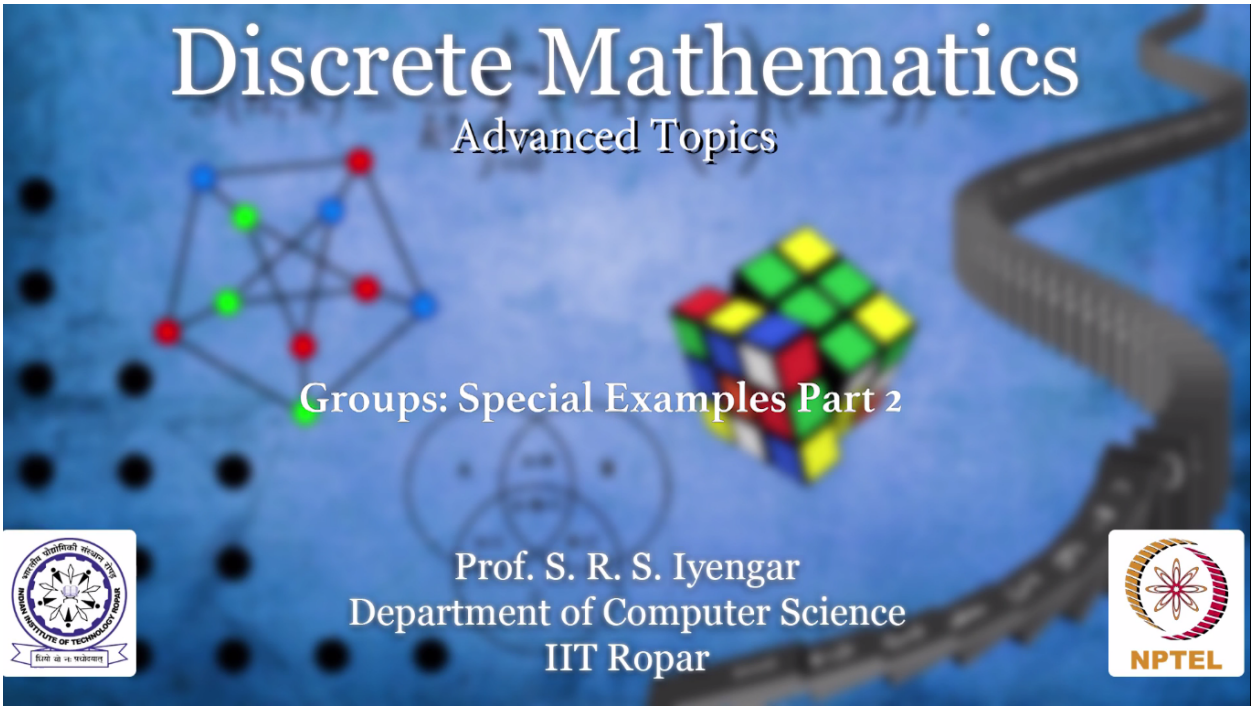
Discrete Mathematics

Functions

Advanced Topics



Groups Special Examples Part 2

Prof S.R.S. Iyengar

Department of Computer Science

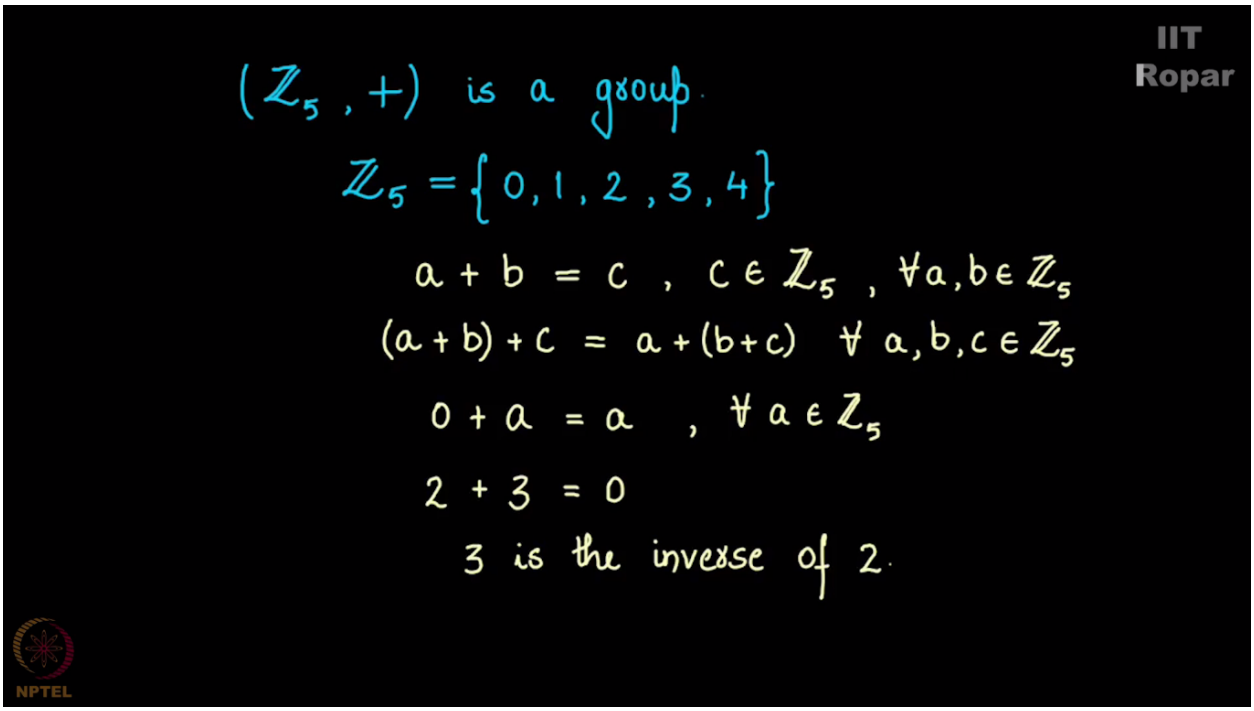
IIT Ropar

In the earlier video I had told that Z5 is a group under addition modulo n. Let us see how.

So Z5 under addition is a group. Let me state it. Now what are the four properties that it must satisfy this set Z5 for it to be a group? First is the closure. So Z5 has these elements 0, 1, 2, 3, 4 we know that . So in general any Zn let me just tell it for your clarity has the elements 0, 1, 2, 3 up to n minus 1. How we got that I have explained in the previous video. Now if I take two elements A plus B I am adding them I get a number or an integer C which again belongs to Z5. How do I do this? I take 1 and 2 I add it. What is it? 3. 3 belongs to Z5. Now if I add 2 and 4 it has 6 but I must divide 6 by 5 and the remainder happens to be 1. 1 belongs to Z5 therefore you take any two such integers A and B belonging to Z5, add them you will get another integer which again belongs to Z5. Now once this is clear associativity must not be a big problem. I add A and B and add another number you see that it will be equal to adding B and C and then adding A to it. You can clarify that by writing it down on a pen and paper.

Now this is true for every ABC belonging to Z5. What comes next is the existence of an identity in this set. So if I take 0, add it to any other number belonging to Z5 I get back that number A itself this is true for every element belonging to Z5. 0 is hence called the identity. Now I am writing 0 here doesn't mean it is only 0. It can also be 5. If I if I add 0 and 5 I'll again get 5. 0 added with any number will give me back the same number. What is an inverse here? Let us understand that what is that number which when added to 1 gives me 0. What is that? If I add 2 I'll get 3 not 0. If I add 3 I will get 4 not 0, and now if I add 4 I get 5. 5 divided by 5 gives a remainder 0 and hence 4 is the inverse of 1. 1 is the inverse of 4; both ways it is true.

Now what is that number which when added to 2 leaves a remainder of 0 when divided by 5? The statement was very lengthy you might want to pause and watch it again. If I add 3 to 2 I am going to get a 5. 5 when divided by 5 leaves a remainder 0 and hence 2 is the inverse of 3 and 3 is the inverse of 2. It's an addition here and hence all these explanation will hold true.



So we have seen that every element has an inverse. I have not explicitly mentioned about 0 it is very obvious that 0 is itself the inverse of 0 and hence Z5 under addition is a group. It is integers modulo 5. In general it is true for any n. Zn under addition modulo n is a group. Now you can try it out for Z2, Z3, for any n.