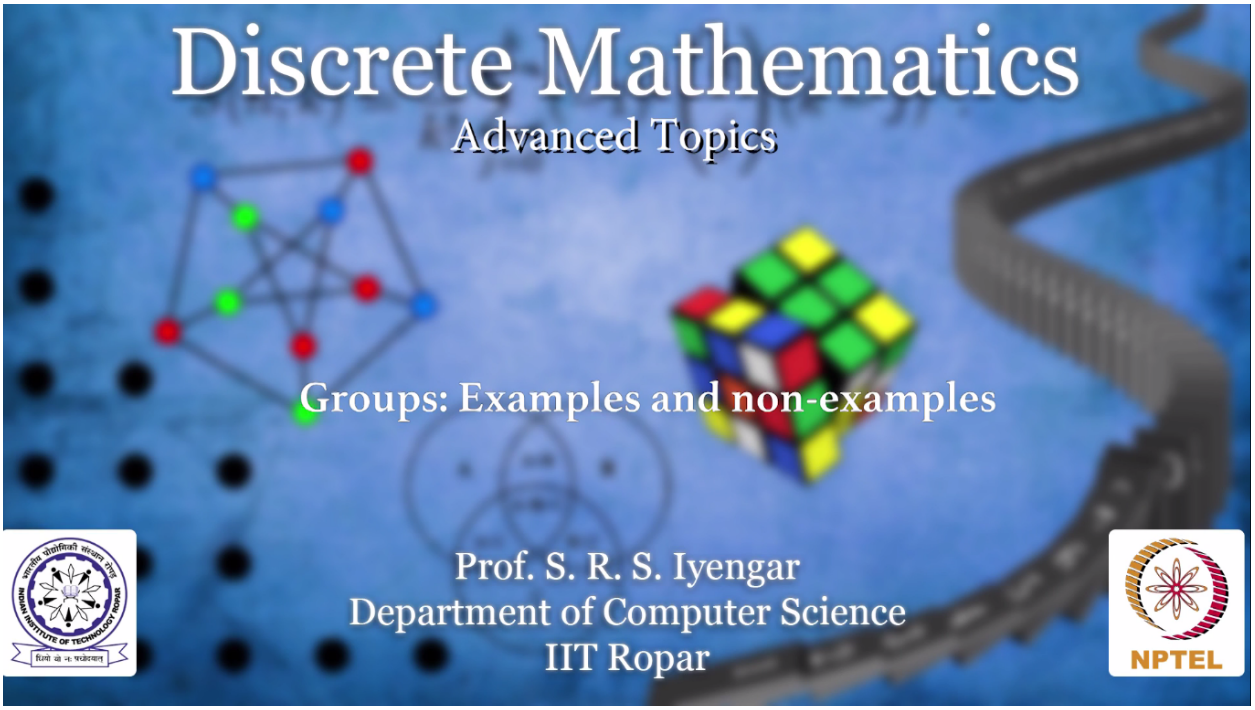
Discrete Mathematics

Functions

Advanced Topics



Groups Examples and non examples

Prof S.R.S. Iyengar

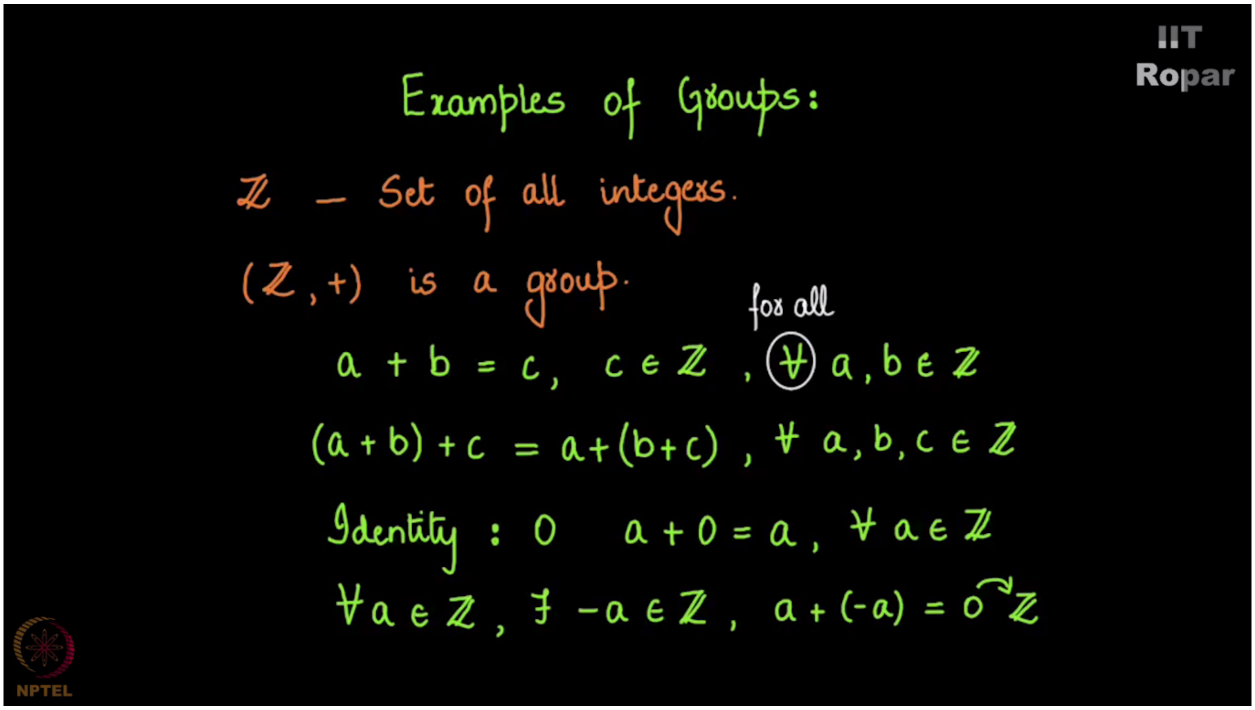
Department of Computer Science

IIT Ropar

Let us now see some examples of groups. Also some non examples to understand the difference when set is said to be a group and when it is not. Let me start with some examples okay and the first one I'm going to take is integers. The set of all integers. Consider Z under addition. What do I mean by that? I am going to consider the set Z and the binary operation is going to be plus addition. Now this is a group. Let us see how. You take any two integers A and B. Add them you get C where C is also an integer and this is true for all A and B belonging to integers. You take any two integers when you add them you're going to get another integer.

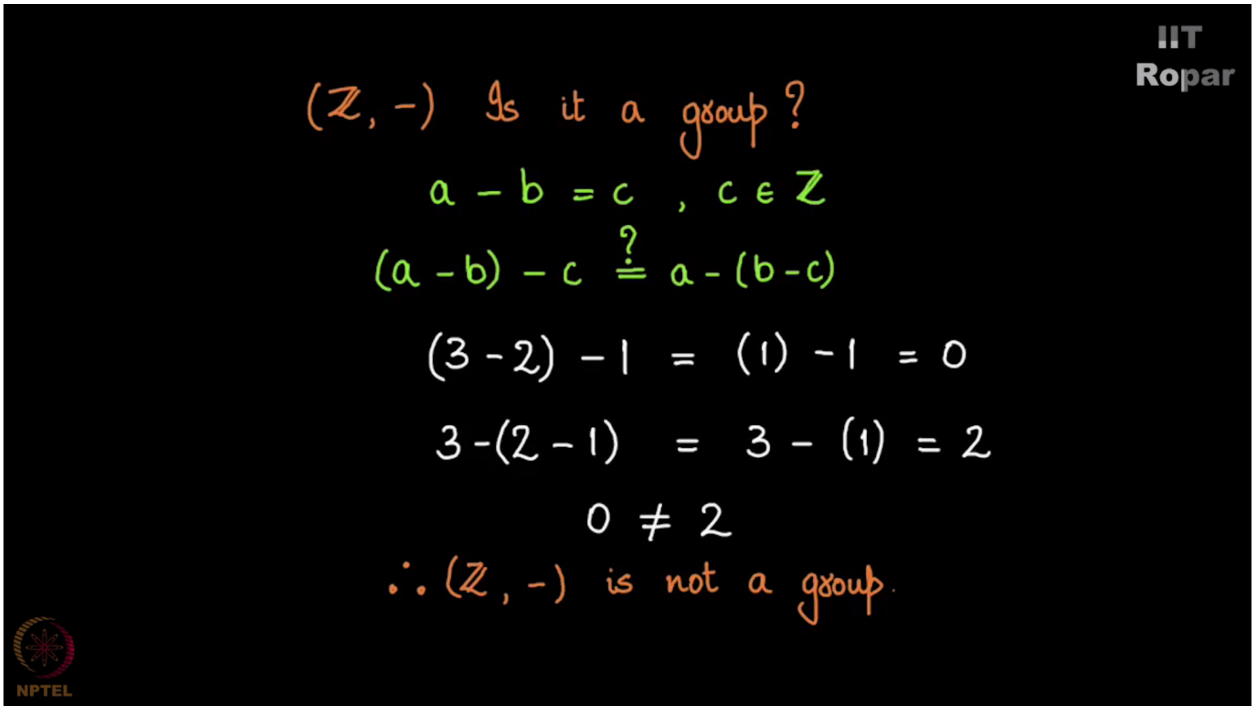
Now you take two integers well the symbol represents here for all. You have seen this in the logic chapter we are going to use this more frequently now. You take any two integers, add them you get an answer you get an integer now add C to it. Now it will be equal to adding B plus C and then adding A to it. Well A plus B if you are then add an integer it is same as adding B plus C and then adding A to it and this is true for all ABC belonging to Z. This is a property which integers satisfy.

Now what is the identity here? It is 0. Why? For every A in the group that is the integers when you add 0 to any integer what do you get? You get back the original integer. This is true for every A belonging to Z. Now which is the last property for every integer A in Z you have minus A there exists minus A belonging to Z such that A plus minus A is zero and where does the 0 belong to? It belongs to Z. This 0 is what we spoke of in the previous property it is the identity.

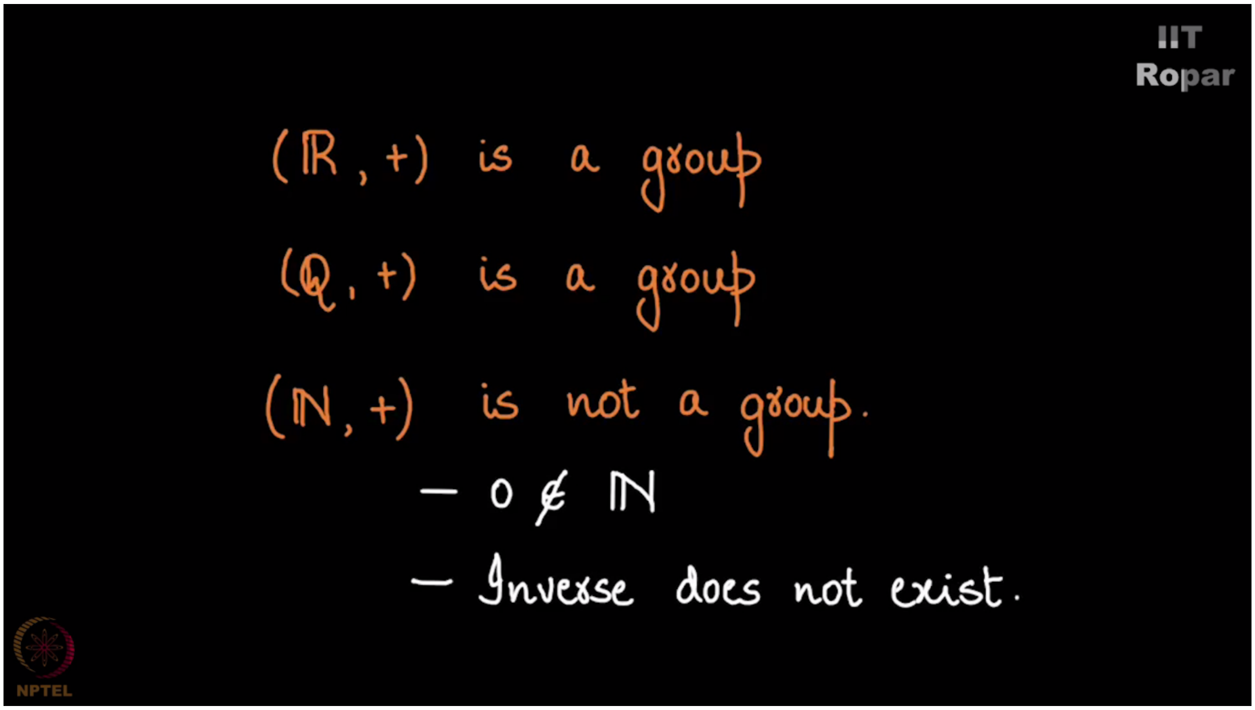


So you take an integer the minus of it, the negative of it is the inverse of that particular A. So Z plus is a group. It satisfies closure, associativity. It has an identity and it has an inverse. So Z plus is a group.

Now is Z under subtraction a group? Let us see. A minus B when you do you get C. When you subtract two integers you get another integer and this integer C is also in the set. Now when you subtract A minus B and subtract an integer to it, is it the same as subtracting B and C and then doing A minus to it? Is it true? Let us see. 3 minus 2 I am going to do this where see here A is 3 B is 2. Now I am going to subtract 1 to it. C is 1. What do I get. It's 1 minus 1 which is a 0. Now is this the same as 2 minus 1 and then doing 3 minus 2 to it which becomes 3 minus 1 which is 2. Do you see 0 is not equal to 2 and hence Z under subtraction is not a group. You see the second property itself is violated. We need not check the rest of it that is identity and inverse. We need not go till there. Closure is satisfied but associativity is not and hence this is not a group; which one? Z with subtraction.

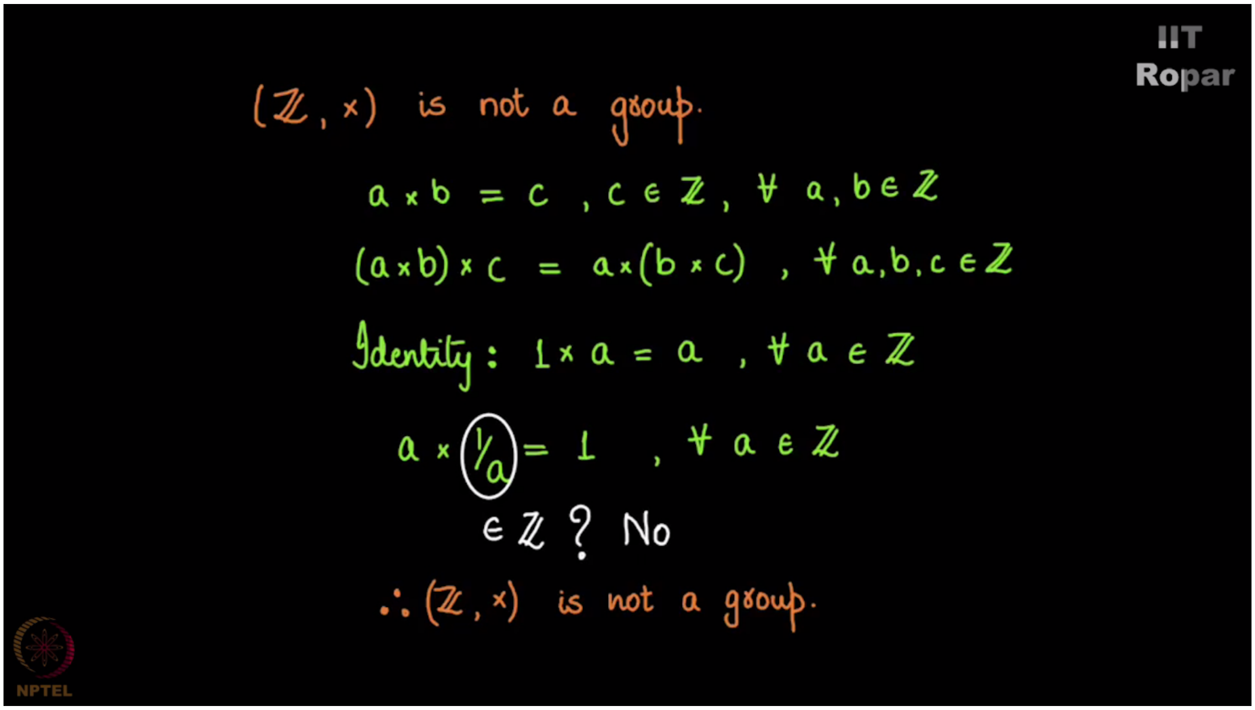


Here are a few more examples. Real numbers under addition is a group. You can verify the properties yourself by sitting with a pen and paper you can check that closure, associativity, identity and inverse satisfies. Under addition identity is always 0 and inverse is always the negation of that particular number. Rational numbers under addition is a group. Q plus and natural numbers under addition is not a group. Why? Because 0 does not belong to natural numbers and what is 0 it is the identity. It must belong to natural numbers. Since it does not belong natural numbers are not a group. Also universe does not exist. What is the inverse? Negation of that. We have negative numbers and negative numbers do not belong to natural numbers and hence natural numbers under addition do not form a group. We have seen about an addition.



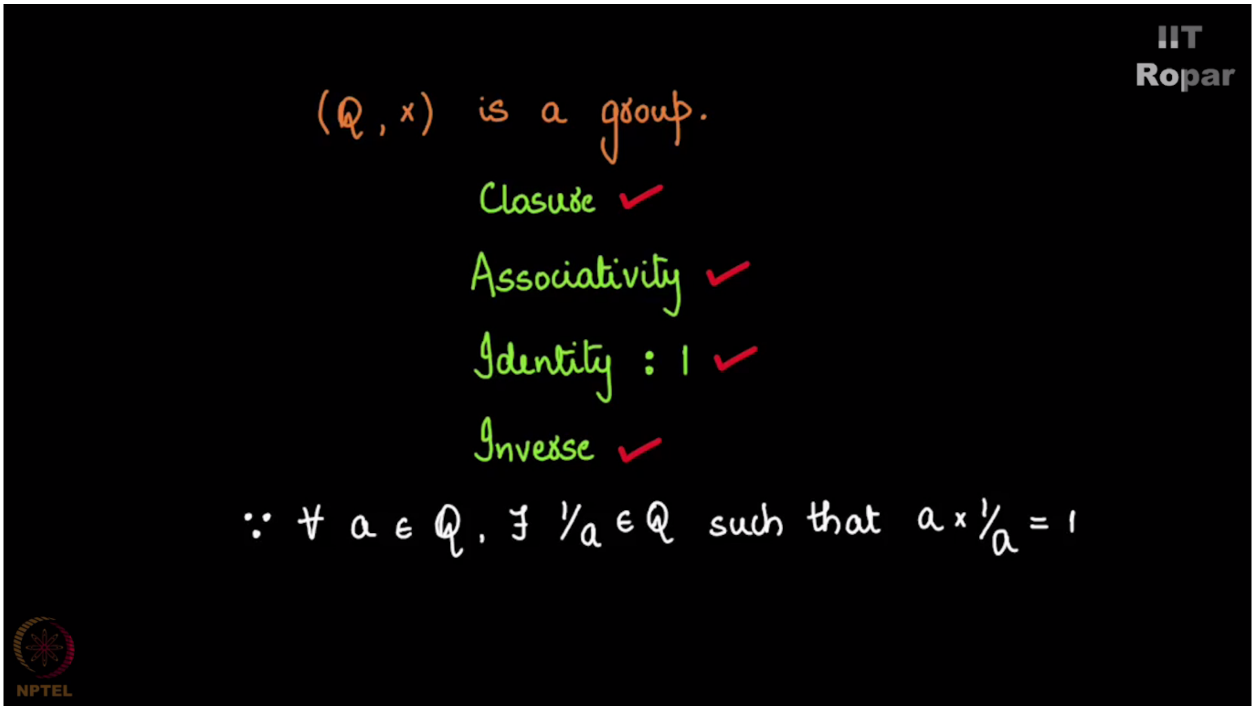
Now let us see multiplication Z under multiplication is not a group. Why? You multiply two integers you get another integer C. C also belongs to Z and this is true for every integers A and B belonging to Z. Now closure is satisfied. Let us see which is that property which is not satisfied. You multiply A and B and multiply C to it it is same as multiplying B and C and then multiplying A and this is true for all ABC belonging to Z. So associativity is satisfied. Closure is satisfied. Associativity is satisfied.

Now what is the identity here? Well identity is one. How? You take an integer A multiply it with 1 you get A back. A number multiplied with 1 gives you back the same integer and this is true for every A belonging to Z. Hence, 1 is the identity. Now what about inverse? Does inverse exist? Let us see. What is that number which when multiplied with A will give you one? What is that number? That number is 1 by A. A and A gets cancel and you get 1 but this does not belong to Z. For every A this must be true. For every A you must have 1 by A which when multiplied with A will give you one but this 1 by A does not belong to Z and hence inverse does not exist and Z under multiplication is not a group.



You might want to pause the video and watch it once or twice.

Let us see if Q under multiplication is a group. Yes it is. how? Closure, associativity, identity is 1. Inverse will also exist. Closure is true satisfied. Associativity satisfied. Identity is 1 satisfied. Inverse is 1 by A that also exists because for every rational number belonging to Q there exists 1 by A belonging to Q such that A into 1 by A is 1 and hence it is a group. R under multiplication is a group. Real numbers. It is a group.



Now I have a question for you all you can take it as an exercise. We have seen how addition operation is playing a role here in making a set a group or not. We have seen how subtraction plays a role. How multiplication plays a role. Now the question for you is is Z under division a group? So you might want to check all the properties one by one and see if integers under division will form a group or not.

Once you know about integers you can go on and verify if R under vision is a group are not, rational numbers under division is a group or not.

$(\mathbb{R}, \times)$ is a group.

Q: Is $(\mathbb{Z}, \div)$ a group?