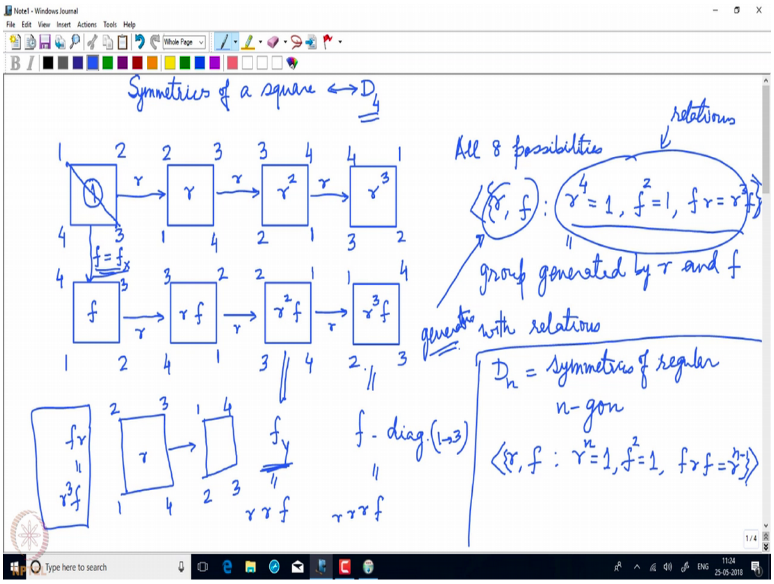
Groups: Motion, Symmetry & Puzzles
Prof. Amit Kulshrestha
Department of Mathematical Sciences
Indian Institute of Science Education and Research, Mohali

Structure of groups
Lecture – 06
Generators and Relations

(Refer Slide Time: 00:14)



So, welcome back, we in the last lecture saw some puzzles, the came with the marble peg, solitaire, 15 puzzle and now we are moving over to Rubik's cubes and to understand Rubik’s cube there are few more things that one has to understand how to solve a Rubik’s cube using ideas of mathematics, ideas of group theory because Rubik’s cube as I said is the playing Rubik’s cube is just permuting certain small cubes right. So, everything noise about a generators and relations so, what are the results for the relations and how you can present you, how can you express a group, as generators and relations that is what we are going to learn.

So, for that we begin with an example and you have already seen this example in one of the earlier lectures and this example is about symmetries of a square and as I said now in previous lectures that they form a group the group is called D for 4 strains for 4 sides of the square. So, let us see what are all the symmetries of a square I take this as identity position 1 2 3 4 that is identity position, r stands for rotation by 90 degree in anti clockwise direction and f stands here for flipping about x axis.

So, accordingly I am going to label all these configurations all these configure configurations of a square. So, they rotate by ninety degree what happens to 2, 2 goes to this position to comes here. What happens to 1, 1 comes here, what happens to 4, 4 goes there and 3 comes here. So, we have like this once again I rotate this configuration by ninety degree and what do I have one comes here this time this side. So, I have 1 2 3 4 and once more this time 1 goes here and I have 1 2 3 4 so, there are 4 positions.

So, first 1 is here, then 1 is here, then 1 is here, then 1 is here, similarly similarly you have other configurations. Now what happens when you flip about x axis so, what did I say x axis I am flipping. So, 1 comes here, 2 comes here, 4 comes here and 3 comes here and after flipping I am again doing what I did earlier I rotate by 90 degree. So, this time 1 goes here. So, I have 1 2 3 4, once again 1 2 3 4 and once more so, this time I have 1 here, 1 2 3.

So, here I have obtained all these considerations on this square just have to check that these are all 8 possibilities there are no other there are no other possibilities. So, this I denote by identity 1, this I denote by r, this I denote by r square, this I denote by r cube, what about this 1 here I do first f. So, this is a f. So, this is what, this is I first to f and then r f, r square f, r cube.

So, like that I have various a configurations, what about flipping about y axis have already covered it let us see this original position and flipping about y axis will be 2 here, 1 here, 3 here, 4 here. So, 2 here, 1 here, 3 here, 4 here it is this one so, this is actually want f y this is f y flipping about y axis similarly I have also covered flipping about diagonal somewhere. So, that is interesting right I did flipping only about x axis and by composing it with rotations by 90 degree I could cover flipping about y axis as right similarly I have also covered flipping about the diagonal.

Let us see how so, one. So, suppose I take this diagonally 1 3 and about this diagonal let me 1 3 will remain here 2 will come this side and 4 will go that side so, 1 3, 1 3, 2 4. So, this is actually a flipping about diagonally 1 3 so in fact, all the possibilities have been covered. So, that is interesting what does it mean; that means, to obtain a y, what you need is f and r and r you first have f then r then r and similarly to flip about diagonally what you need is first flip about x axis f is f x flip about x axis and r then r then r now..

So, next is you can obtain f y from r and f. In fact, all these 8 elements are generated by just 2 elements, f and r rotation by 90 degree in ninety clockwise direction and flipping about x axis and that is how we start calling f and r is generators for the group D 4. So, I have r I have f. So, these are 2 generators just by combining them in certain fashions I can obtain everything in this group and what are the relations.

Relations are if I do r 4 times I rotate by 90 degree 4 times I get back my identity and if I flip about that success twice I get back my identity and then there is some relation between f r and r f let us see what kind of relation it is. So, I have written r square f what about f r. So, let me try to write f r here. So, you have this square I have 1 2 3 4.

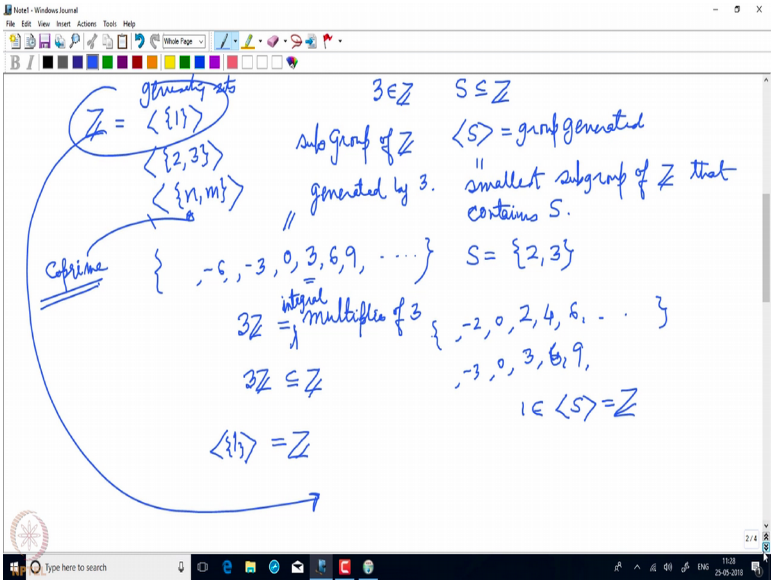
So, after f what will happen no this is a sorry this is all said. So, you have f r here. So, first I write what r is doing, r is doing it 2 3 1 4 that is r you see and then I am doing f, what is that at flipping about x axis so, 1 4 here and 2 3 here. So, there is 1, 4, 3, 2 so, it is 1, 4, 3, 2. So, f r is actually this one f r is actually equal to r cube f. So, these are relations. So, f r is same as r cube f and so, you have this, r f and conditions are these. So, rotation goes like this. So, this is what this is group generated by r and f with relations as expressed here.

So, every group can be expressed in terms of the generating set and relations generating set need not be unique. In fact, in case of taking this f x I could have taken say f y and then the same group would have got generated with those generators. So, I could have used some other set of generators. So, these are generators and these are relations , relations , generators, similarly you can try to think about other generators, other relations in some other groups.

So, if I take the general situation D n, what was D n, D n is symmetries of a of regular n gon then the relations would be essentially similar except for. So, r f where r to the power n is 1 f square is 1 and then f r f is r to the power n minus 1 so, these are the relations there. In general it is very difficult to determine from generators and relations what exactly is the structure of the book, what exactly does the group look like the same group can be expressed by a different set of generators and different set of relations that is quite that is quite possible.

So, in generally it is a very difficult problem to make a guess about what the group is going to be just by looking at generators and relations there were the less it is quite important in mathematics to understand it is quite important in theory of groups to understand what are variations in a group and it is always desirable to find the maximal set of relations.

(Refer Slide Time: 13:38)



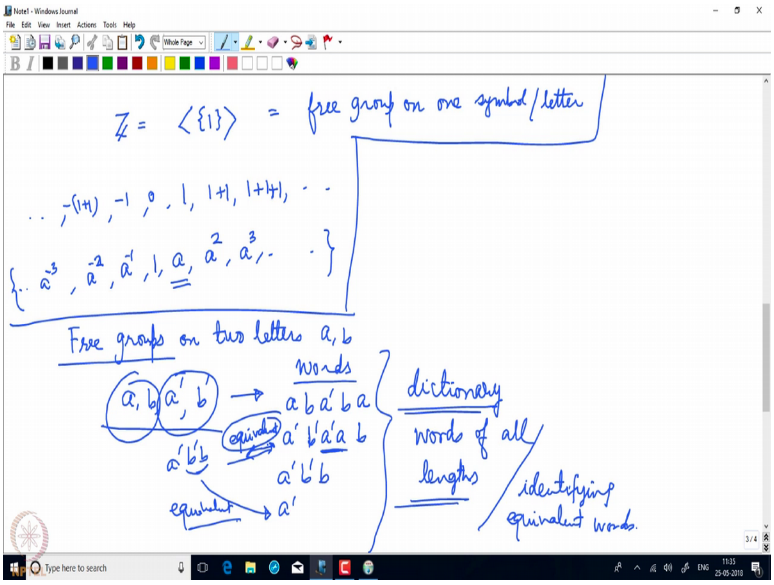
Let us let us take few more examples the easiest example actually now, what about Z. So, if I take some element in Z, I take 3 if I take this element 3. So, I can ask the group or rather the subgroup of Z which is generated by 3. So, if 3 is there, 3 plus 3 6 has to be there, 9 has to be there and so on, of course, the group 0 has to be there, 3 is there, minus 3 has to be there, since 6 is there, minus 6 has to be there like that.

So, subgroup of Z which is generated by 3 eventually turns out to be these are multiples of 3 integral multiples of 3 these are integral multiples of 3. So, 3 Z integrals in multiples of 3 that is a subset of Z, but if I take 1 so, if I take 1 and the group generated by 1. So, for any subset as in Z this is group generated, what is the meaning of group generated, the smallest group which contains S, so this is smallest subgroup of Z that contains S.

So, if I take 1 then it is equal to Z. So, 1 is the generating set of Z; however, I could have taken as to be say 2 and 3 , see if 2 is there, 4 has to be there, 6 has to be there, and all that 0 has to be there, minus 2 has to be there, in like that and since 3 is there all multiples of 3, 3 6 9 all of them have to be there as I said, but then since 2 is there, in 3 is there, the difference of them also has to be there. So, 1 also has to be there in the subgroup generated by S and since 1 is there the subgroup generated by S the subgroup deleted by is actually Z.

So, there are various generating sets for Z. So, Z is generated by say 1, Z is generated by say 2 3 or you take any co prime integers n and m co prime then. In fact, they are going to generate Z as a group. So, there is no uniqueness in the set of generators of a group, now think of this Z as you read it by 1.

(Refer Slide Time: 17:58)



So, Z is generated by 1, where are the relations, what are the relations. So, since 1 is here, 1 plus 1 is here, 1 plus 1 plus 1 is there and so on and the 0 has to be there as I said minus 1, minus of 1 plus 1 and so on , there is no relations in Z and just a way to say it is to take any symbol a. So, in the group which is related by a, a square is there, a cube is there, and so on identity element is there, a inverse is there, a to the power minus 2 is there, a to the power 3 is there, and so on. So, there are no generators, there are no relations generator is of course, singleton a, but there are no relations. So, Z is therefore, called free group on one symbol or one letter.

So, when we do not enforce any relations what you have is free group, free group has much more abstract definition, which is in terms of certain universal property, but in these lectures you are not going to be bothered about the definition. So, let us understand a free groups so, what I have is, to start with free groups on 2 letters. So, those 2 letters are a and b just 2 symbols. So, any combination of a and b has to be there in the free group and then there are no relations.

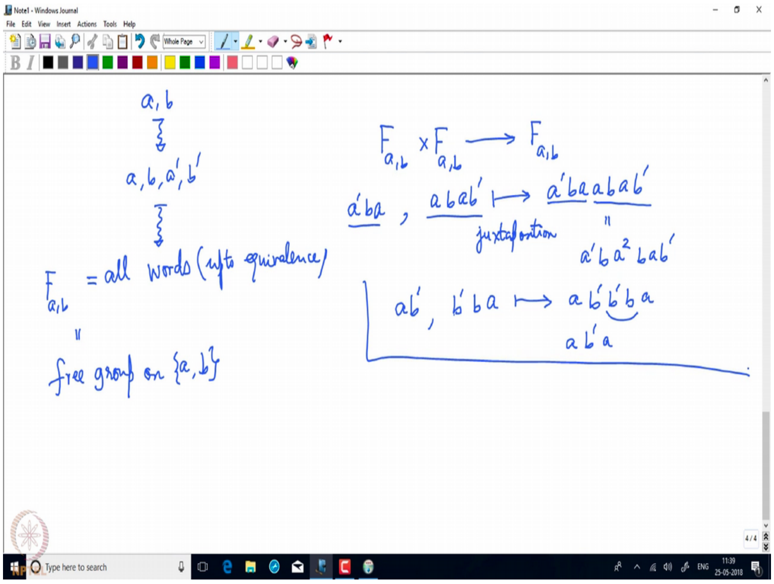
So, how do we go about, a is there, b is there, I introduce 2 more symbols a prime and b prime and then I consider with these 3 4 symbols with these 4 letters I need words. So, how do words look like, any sequence of them any sequence of a b a prime b prime and in any fashion of any length. So, see a b a prime b a that is one, a prime b prime a prime a b that is one, a prime b prime b that is one, a prime that is one. So, there are so many words which are they, which are there.

So, what am I doing with these 3 4 letters I am constructing actually all possible words of all possible names. So, I am having dictionary of these words. So, I am constructing a dictionary out of all these words. So, words of all lengths and here I would be skeletally careful because I have talked about groups, group relations, the group axioms should be satisfied and it should be clear why a prime and b prime are introduced. So, what I would say I would say that whenever a and a prime occur in a in the world back to back or being b prime occur in the world back to back then I will just collapse them and then I would say that after collapsing that this is a prime b prime b.

So, this word is actually equivalent to this world, sequin entities this word and again b prime b are coming together, they will collapse and then this is equivalent to a prime ok. So, I am considering words of all length and I am just being careful that I am identifying equivalent words equivalent words ok. What do I have now, I have I started with just 2 letters a and b, I put 2 more words 2 more letters a prime d prime, and a prime was introduced..

So, that a prime can act as inverse of a and p prime was introduced because it wanted something to act as inverse of b and keeping that spirit we created the definition of equivalent. So, that whenever b prime b being b prime come together or in a prime come together I collapse it. So, just from 2 letters I can create huge connection so, I have all this dictionary.

(Refer Slide Time: 24:30)

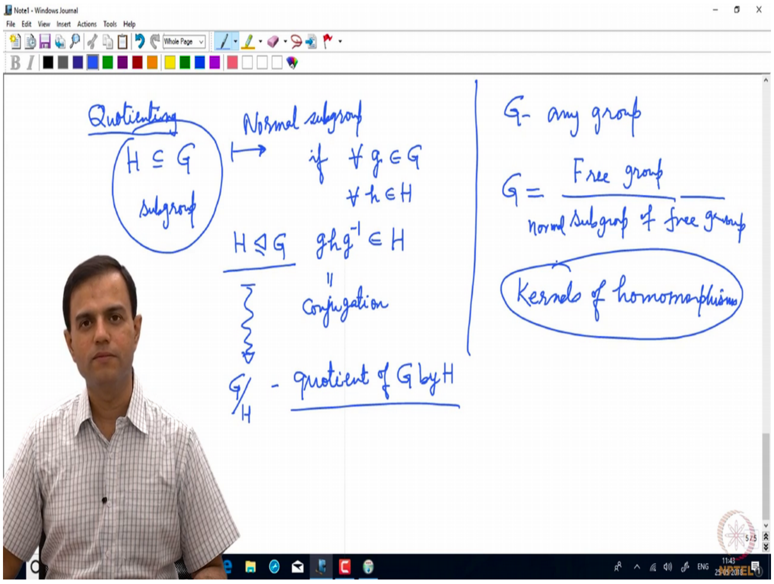


So, from a prime b so, from a b, I have a, b, a prime, b prime and then I have all words up to equivalence meaning the 2 equivalent words there were 2 words which are equivalence I am going to treat them same. So, this collection is called f or f a b which is free group on a b, how big is this group? It is huge it is infinite group it is really huge and how do I take group operation in this group, I just take a word save a prime b and here I have some word a b a b prime some word. So, what is the composition where it is a group low on them just a position you just place these 2 words back to back, place first word, then you place second word, just merge it the formally fashion, what is that, a prime b a a b a b prime right a prime b a and a b a b prime.

So, simplified form of this would be just a notation a prime b when you have a and a back to back it is notation is a square and then b a b prime. If there are some other words say if there was a b prime here and if b prime, b were here while b prime b is identity will b prime b a over here, then what would I do I would just simply consider the composition of them as a b prime, b prime b a. So, I would just dissolve it I would just say b prime b is identity. So, this would be just a b prime a right.

So, whenever you have a and a prime of a b prime just going to collapse it. So, this is how free groups work, one query that you may have is what are they good for, the construction looks. So, abstract just having 2 symbols to letters and from those 2 occurs you are constructing huge group what up what is the advantage of having such definitions maybe it is use for abstract mathematics is there any application of this beyond it beyond this construction when we discuss Rubik's cube I will show you how useful is the concept of free groups, few more words before I stop here is a notion of cosine thing which I am not going to make very precise.

(Refer Slide Time: 28:27)



So, whenever you have a group G and whenever you are having a subgroup H is a definition it is normal subgroup. So, this set up H subgroup of G we you would called normal subgroup. If you pick any element of g and any element of h and you consider g h g inverse this is so called conjugation, you are conjugating g h g then that should also belong to G sorry that should belong to H.

So, if H has this property then it is called normal subgroup and the notation is H is normal subgroup of G and whatever your normal subgroup to this you associate another group which is G mod H the notation is called quotient of G by H. So, you are having some quotient of G by H, I am not going to define it, but some words I am saying. So, one can think of the time comes maybe I would explain it in detail if you have any group G then I can express G as a free as a quotient of free group by some subgroup some normal subgroup of free group.

So, all the subgroups are going to arise naturally when we homomorphisms, isomorphisms in previous lectures I just briefly mentioned the word homomorphisms is an isomorphism, but normal subgroups are going to arise when we talk of kernels of homomorphisms, when we discuss Rubik’s cubes kernels of homomorphisms are going to play the important role.

So, we should see all that in the next lecture keep watching I hope you are enjoying all this.

Thank you.