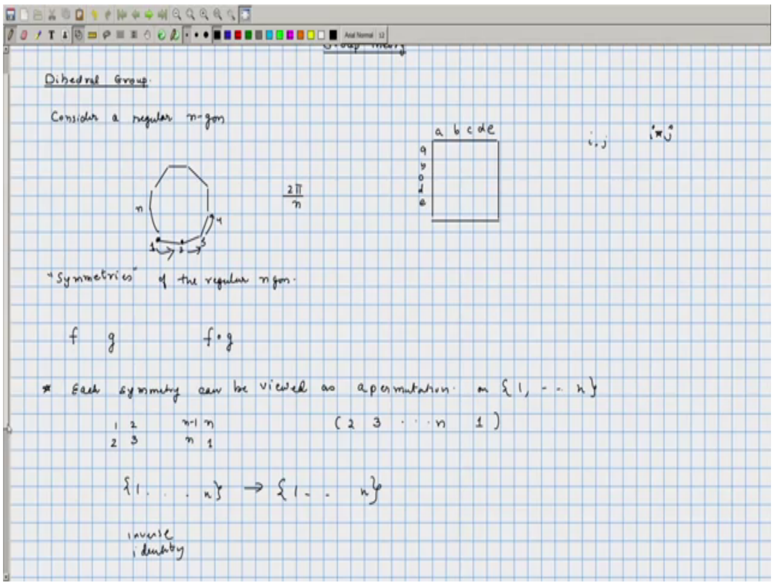
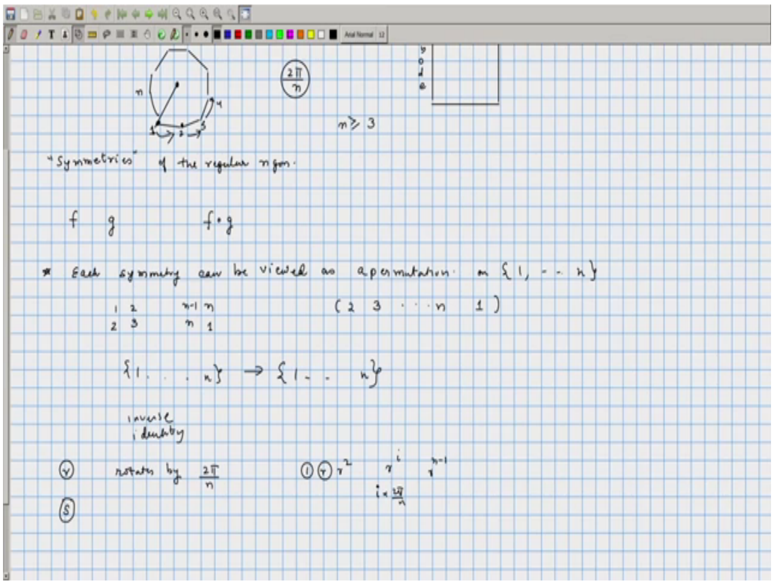
Discrete Mathematics
Professor Sajith Gopalan
Department of Computer Science and Engineering
Indian Institute of Technology, Guwahati
Lecture 39
Dihedral Groups, Isomorhphisms

(Refer Slide Time: 0:32)





So we had seen many examples of group, today we will see one more example, a special group called as the dihedral group while we are studying this group will also learn that this is non-commutative group. We will learn the concept of generators and how a group is presented or described.

So let us understand what is the dihedral group is? So consider regular polygon having n vertices, so let us think that in r2 in the two-dimensional plane there is a polygon with n sides, it is a regular polygon. We are interested in symmetries of this polygon, by symmetries what we mean is all those rigid motions which will leave this polygon in the same location it will leave the polygon unchanged. Here we have given labels to the corners of the polygon but when we are talking about the regular n-gon we do not really labels the vertices, label vertices for a reason that will become clear shortly.

So we want to look at all those motions, all those rigid motions which will leave the regular n-gon unchanged, one such motion would be let us say if there are n sides and if we rotate this n-gon by an angle 2 Pi by n that is the angle in radiance rotate by this much amount, rotate about the centre of the regular n-gon then the starting configurations, ending configurations would look identical okay ofcourse if you have labelled the vertices then whatever was at vertex1 will go to vertex 2 if our rotations where anti-clockwise, so that is an example of a rigid motion which leaves the n-gon unchanged.

So let us consider the collection of all such rigid motions of this regular n-gon, so fix an n so let us say n is equal to 8 or 10 I mean pick any number and consider a polygon of those many regular polygon of those many sides and we are interested in set of all the rigid motions which will leave the n-gon or the inside polygon unchanged, if you look at this collection, does this collection form a group and if so under what operation?

Since your, we can think of these motions as rigid motions as functions with a transforming one point to our changing one point to another, we could think of function compositions as the natural operation. So, suppose S is a rigid motion, it means it is changing (I mean) it is taking the polygon then moving it around in the 3D plane in R3 and finally it is placing it in some particular way in I mean on the plane and the diagram looks exactly the same that is what we mean by symmetry.

So if you have one such and if you have g, if you do the operation of g and then follow it by f that can be written as f composed with g, so it means you do these operations together then you can reason out that the resultant operation will also leave the polygon unchanged, those one operation which left it unchanged on the resulting thing which is the same as the original one again apply another operation and that would give you back the original polygon itself and therefore if you combine 2 of them, they will naturally be a symmetry.

Now how do we describe these symmetries? We could ofcourse think of them as maps from R3 to R3 but that is a huge object means you are mapping every point from R2 to some point in R2 when you have given the function. Okay but here what really matters is where is the vertex 1 being sent to? Okay, so we can in fact represent every symmetry of the regular n-gon by means of a permutation, okay.

The permutation decides I mean if one was this particular vertex after the rigid motion this vertex has to end up as some other vertex, which vertex is it? Vertex 2 has to end up in some other place in one of these other vertices, where does it go to? So each symmetry can be described using permutation, so that is a key observation.

So here we are looking at symmetries of the regular n-gon, so if you fix the polygon and then every symmetry can be viewed as a permutation on the set it is 1 to n, so label the vertices as polygon as 1, 2, 3 up to n and then we can look at permutations over or arrangement of 1 to n over these and each rigid motions which is a symmetry can be viewed as a permutation, so in fact the rotation by 2 Pi by n radians would be the permutation which maps (1 to 1) sorry 1 to 2, 2 to 3 and n back to 1, so n minus 1 would go to n and so on, so 1 goes to 2 and 2 goes to 3 and 3 goes to 4 and so on, okay.

So if you look at the permutation given by 2, 3 up to n followed by 1 this is a permutation which encodes or which this permutation represents the symmetry that is obtained by rotating the n-gon by an angle 2 Pi by n, so now we have just done just one example, one of the symmetries can be viewed in this way, you can convince yourself that every symmetry can be viewed as a permutation (okay, now) and therefore the collection of symmetries is going to be a finite set.

So this is an example of a finite group (okay) but the simplest way in which this group could be described or any group could be described, any finite group could described is by means of what is called as its multiplication table, so if a, b, c, d, e are the elements we have a matrix index by a, b, c, d, e we have a square matrix and at each position, at the position i, j we will give the value of combining I with J.

So i star j will be written at the position i, j in the matrix, such a matrix is known as a multiplication table, so here in an abstract sense we know that take all the symmetries of this regular n-gon you get a collection and these collection (())(8:55) property that 2 of them can be combined by means of function composition, if you give them as permutations, permutations are again functions from 1 to n to 1 from the set, 1, 2, 3 up to n to 1, 2, 3 up to n, so these functions can be composed and that operation basically is an associative operation, so function under function compositions, the requirements for the set symmetries to be group is satisfied.

Required properties where first is closure that means 2 elements should combine and give an element in the collection that is ofcourse the case and it is associative you can verify that and the remaining properties where inverse, the existence of an inverse, so if you look at any permutations, it has an inverse permutation and that inverse permutation will basically correspond to a particular symmetry.

Okay so you are basically reversing if 1 was sent to n look at the permutation which sends n to 1 okay and the symmetry corresponding to that is the inverse is the symmetry that we are interested in and the permutation which maps every element to itself or the identity map will serve as the identity okay, so inverse and identity properties that are required of groups have also we have checked those as well, okay.

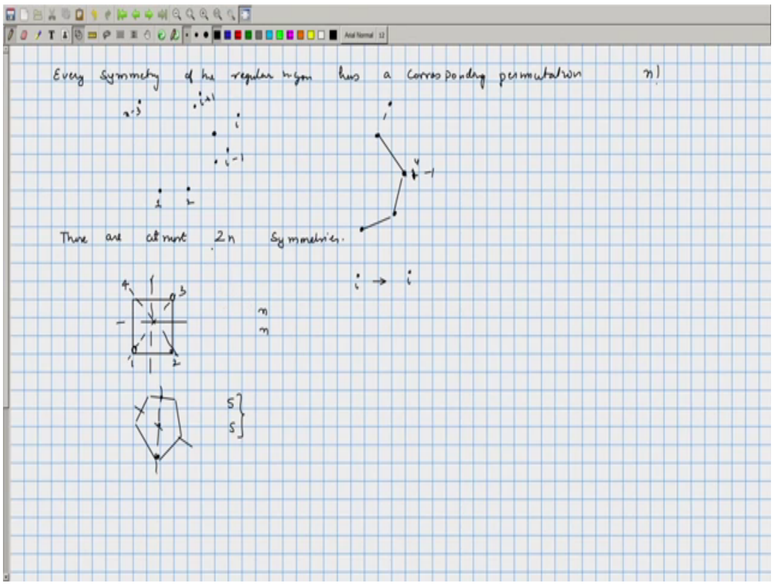
So this forms a group okay that is is clear from an abstract sense but can be present this in a more concrete manner. Okay what are all the elements, can be lead out can you innumerate it? Okay, so we will show that if you take the regular n-gon, we will assume that n is let say greater than or equal to 3 because 2 sided polygon really does not make much, means it is not very meaningful quantity, so we will consider that n is greater than or equal to 3 for all these discussions that we going.

So let us look at any polygon and will look at the special object wherein we are rotating by 2 Pi by n. Okay let us call that as let us R okay, so R is a symmetry or the operation which rotates by 2 Pi by n okay, so if you look at these elements 1 r, r square r raise to n minus 1 they are all symmetries, so one means do not do anything or the identity symmetry and r is rotate by 2 Pi by n, r square is rotate by 2 times 2 Pi by n, r raise to i is rotate by i times 2 Pi by n and so on.

So these are some of the symmetries, are there most symmetries for the regular n-gon? So let us introduce one more symmetry which is, we will call by the name s, which is, so by s we mean the symmetry which looks at the line joining let us say 1 to the centre and flipping about that point, so s is the special symmetry which is obtained by looking at the vertex, the line joining vertex 1 to the centre and flipping it by that.

In some sense the full collection of symmetries can be described using R and S okay, why is this so? So how many symmetries can the regular n-gon have?

(Refer Slide Time: 13:13)



Okay, so let us since we agreed that every symmetry can be described by a permutation, so every symmetry of the regular n-gon has corresponding permutation and because of this reason we know that the total number of symmetries is going to be at most n factorial, it is going to be much less than that in our case. Since it is described by a permutation if you look at vertex 1 and where does vertex 1 go to, does it go to vertex i, does it go to vertex n minus 3 and so on, so that is one information that we would need.

So let us say 1 goes to some location, okay now if 1 go to vertex numbered i then 2 being neighbour of 1 in the original configuration after you have sent 1 to i, 2 should be sent to either i plus 1 or i minus 1 okay, that is the only possibility because anywhere else you have affected the rigidity of the polygon, so where the motions is no longer a rigid motion, okay.

So there are only 2 options for where vertex 2 can land up, further if you have decided what, mean to which vertex does 1 go to and which vertex does 2 go to, once these have been fixed every other vertex its position will be fixed, if 1 has gone to some position let us say i and 2 has gone to let us say i minus 1, 3 has only one position left and 4 again has only one position left and therefore you can argue that every position gets fixed.

So clearly from this we can conclude that there are at most 2n symmetries, you take any regular n-gon then maximum number of symmetries that it can have is 2n and if you can show, if you can describe some 2n functions, some 2n rigid motions, some 2n symmetries for the regular n-gon we know that that is going to be full set because there cannot be anything outside that because 2n is the maximum possible, okay.

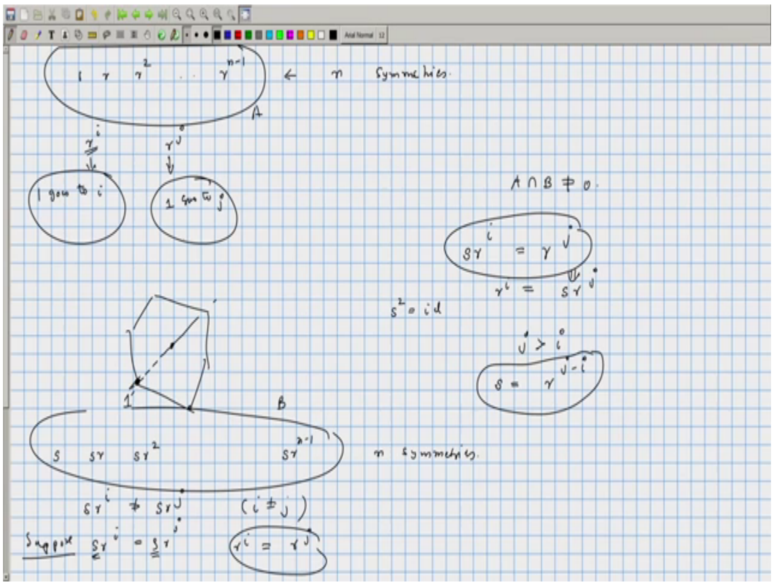
So the symmetries if you want to visualise them, the 2n symmetries they are going to be slightly different for the n equals even case and n equal odd case, okay if you look at the square 4 sided you can rotate by 90 degree 1 will go to 2 that is going to be 90 and 180 means 1will go to 3 okay and (3 will go to) 2 will go to 4 and so on, so that is going to be n symmetries of that kind and you can flip about 4 different axes okay, diagonals and the centre of the sides.

Okay so that will give you additional n symmetries. If this is was a pentagon, okay 5 rotations and then you can flip about each of the vertex and when you join the vertex to the centre it is going to pass to the midpoint of the opposite side, so that is going to give you 5 different symmetries and these symmetries are going to be different because in rotation except for the identity symmetry everything else, I mean all positions will be mapped to a different, I mean there will not be an i such that i maps to i after the symmetry has been applied.

It goes to the image or the position where i lands is going to be different from i okay there is not going to be a single position which remains invariant under the application of the symmetry. Whereas when we flip about a particular axis a lot of elements, means at least more than one elements could remain fixed, so here 1 and 3 are going to be fixed when you flip about that particular axis okay and here when you flip about those axes you can say that there is an exchange within 2 and 1.

Whereas in a rotation there is no exchange of elements, the exchanges are all going to be I mean they get flipped by more than a distance 2 okay, so you can convince yourself that these are the only symmetries but we will argue about it in a formal setting.

(Refer Slide Time: 18:48)



So let us say one, so let us imagine that r was this particular rotation by 2 Pi n, so 1, r, r square, r raise to n minus 1 okay these are all going to be distinct elements because r n minius if you look at any one of them ri and rj, so one goes to i where as if you apply r to the power j one goes to j, so ri and rj has to be different, so this accounts for n symmetries. Now let s be this particular operation that you get, so if you look at regular n-gon this is the vertex number 1 and this is the centre of the polygon join them, okay.

If it is an even sided polygon this line will pass through another vertex, if it is an odd sided polygon it will pass through middle of another side, does not matter which one is the case. We flip about this particular line and that is what we call as s, okay now note s, sr, sr square all the way up to s r n minus 1, okay these are n symmetries, these n symmetries are also going to be all different that means s, r raise to i is not equal to sr raise to j when i and j are different.

Clearly these are going to be symmetries because the first operations is going to leave, flip about these particular axis that is going to leave the vertices that is going to not affect the it is going to leave the polygon unchanged and if you follow it up by another operation which leaves the polygon unchanged you are finally going to get an operation which leaves the polygon unchanged, okay. Can two of them be equal?

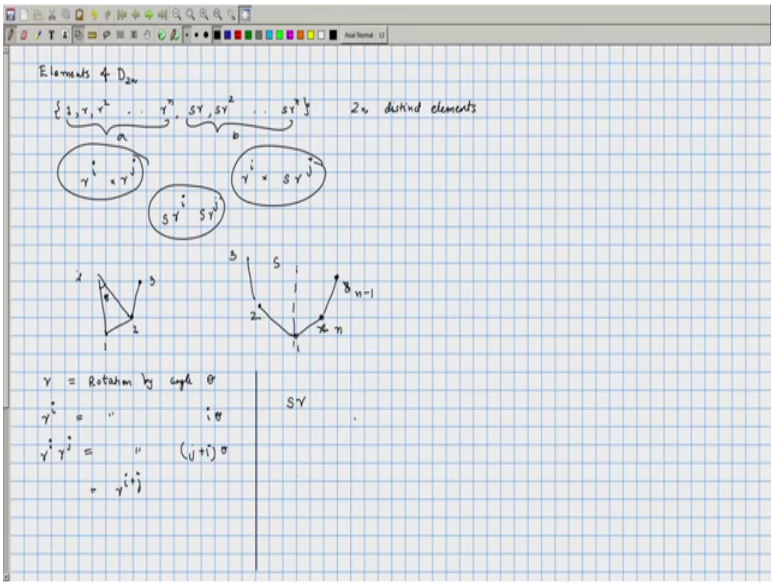
So if sr raise to i is equal to sr raise to j okay, that would mean even if you did not apply this s still things would have been same that means r raise to i will be equal to r raise to j, so this is not the case because we argued that r raise to i and r raise to j are different when i is not equal to j, so here we have n symmetries and here there is another set of n symmetries and they are all different from, these are all different, these are all different but there could still be a problem, could be one element from the set, so if you call this as A and this is B, may be a intersection b is not equal to 0, if a intersection b was 0 then we have accounted for all the elements, okay so let us argue that no 2 elements here are the same, so let us look at suppose sr raise to i is equal to r raise to j.

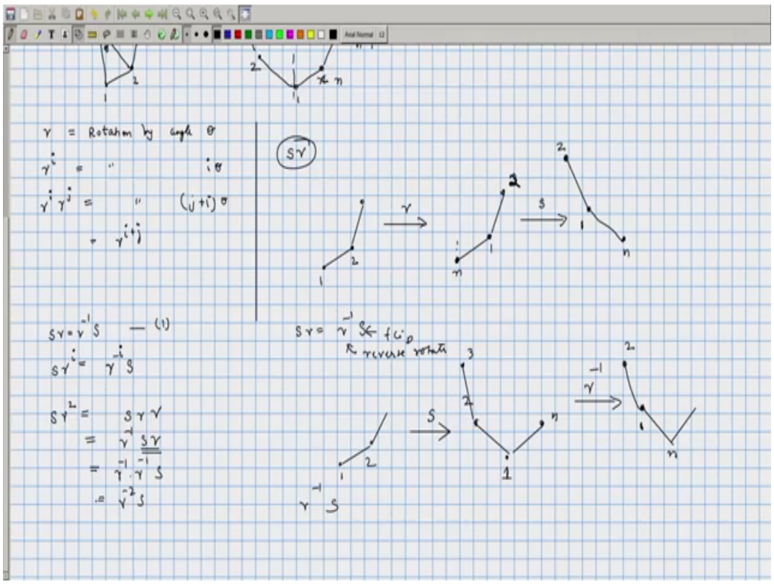
Now if you flip twice that is same as starting permutations that means s square is going to give you identity. So if you have sr raise to i is equal r raise to j then we have r raise to i is equal to sr raise to j, so this statement would imply the second statement by multiplying with s on both sides, so we could assume without loss of generality that j is a larger quantity j is greater that i, so sr raise to i is equal to sr raise to j and therefore we can cancel off.

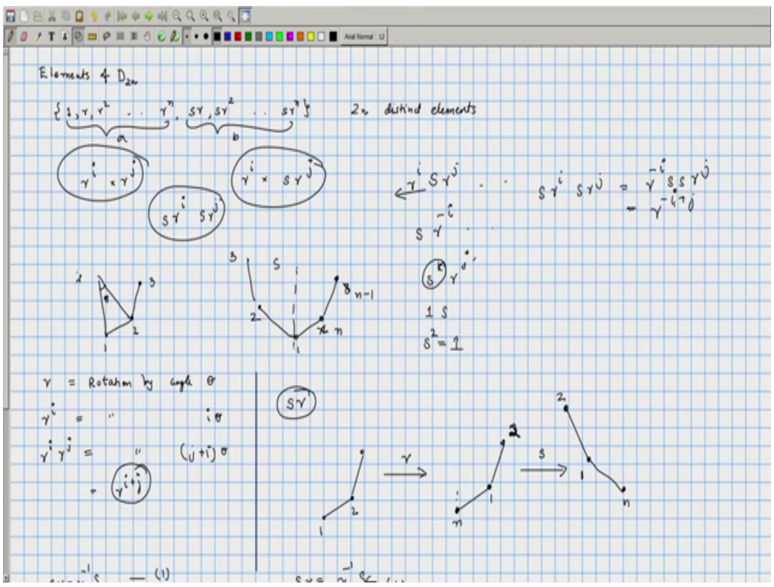
So if we had done rotation by 2 Pi by n times i in one case and 2 Pi by n into j in the other case we can reduce the number of rotations by smaller amount so we can argue that s must be equal to r raise to j minus i okay but this clearly cannot happen, s is a flip r raise to j minus i is some rotation a flip can never be equal to rotation because flip leaves a particular element unchanged.

I mean the vertex about which you are flipping that is here the vertex 1, so flip leaves one unchanged whereas r j minus r raise to j minus I sends 1 to the vertex j minus I, okay so there are no common elements.

(Refer Slide Time: 24:064)







So we argued that the elements of the dihedral group are 1r, r square, r raise to n and sr, sr square up to sr raise to n these are 2n distinct elements, so distinctiveness we have already argued. We also argued that these elements do form a group, now we want to see how this group can be understood in terms of just r and s. Let us try and figure out the multiplication table for this particular group, okay so let us look at general element, identity element how it multiplies it is clear, one multiplies with anything and give the same.

If you have something on from r raise to I, it could either multiply with r raise to j or r raise to i could multiply with sr raise to j or you could have let us say sr raise to i and sr raise to j, so there are 3 types of multiplications that can happen, so if you call these as a and these as b elements of a with itself, b with itself and elements of a with b.

Now r basically was a rotation by some angle theta, so if we thought of the polygon 1, 2, 3 let us just look at how the polygon is drawn and if we find where exactly are 1 and 2 going to after the symmetry is performed that will basically fix the entire polygon and therefore while trying to understand the composition of the symmetries it is enough if we know where the composition maps 1 and 2 into.

Okay so let us say one rotation is by angle theta, so if you call r as rotation by an angle theta r raise to i is basically equal to rotation by i times theta, so r raise to I and r raise to j if you compose it that is equivalent to first rotating by j theta and then rotating by i theta that is equal to j plus i theta, so rotation by j plus i theta and that is equal to ri plus j, so this is a simple multiplication.

Now these 2 have s coming in between the rotations that is flip are coming in between the rotations, so s is basically a flip so if you look at 1, 2, 3 a flip basically about vertex 1 takes this to the other side, so after the flip 2 will be here, 3 will be here and in place of 2 there will be n and in place of 3 n minus 1 and so on. So in order to understand r raise to i times sr raise to j we will first look at the simplest of these, we will look at the simplest of symmetries involving as namely sr, so sr basically means we rotate by r and then do a flip.

Okay, so let us draw this, so we had a rotation so 1, 2 and 3 if we do rotation, when we say sr it means first apply r and then apply s, so that will take 1 to 2 and 2 to the position of 3 and whatever was at n would come to the 1^{st} position and then if we do an s that is flipping about the starting position, so what we will get is n will remain wherever it is and 1 will go to the other side and then there will be 2 1, 2 just above 1, so fixing 1 2 all the other positions gets automatically fixed, okay.

Now can we view this sr as some other expression, so you claim that sr is equal to r inverse s that means first you flip and then you do a reverse rotate, okay so let us try and verify that is the case, so if you look at 1, 2 the initial part of the polygon if we flip that means when we apply an s we will get 1 at the same position and 2 basically goes to the other side and the position of 2 will be taken by n.

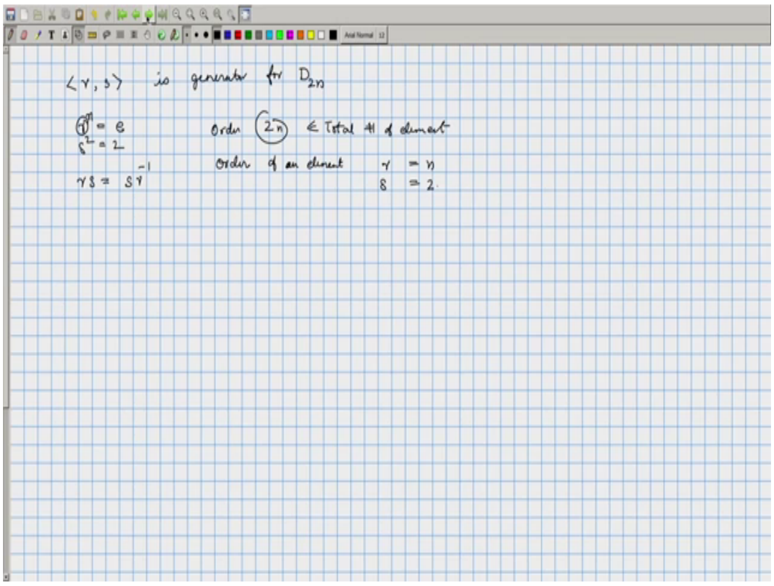
So this is how the polygon will look after we perform an s and if we rotate this by r then the one will go to the position of n but if we do a reverse rotate that is r inverse then what will happen is there will be a clockwise rotation therefore n will come here 1 will come to this position and 2 will go to this position, okay.

So you can see that whatever we obtained by sr is same as what we get by r inverse s, so we can claim that sr equal to r inverse s okay and this would also mean that sr raise to i is going to be r minus i s. It can be seen by repeatedly applying say rule number 1 if you have sr square that is going to be sr r which is equal to r inverse sr and again apply the same rule so you will get r inverse time r inverse time s that is r raise to minus 2 s, okay. So basically what it means is if we have an expression which involves just the r, r raise to I, r raise to j etc we can just to addition and if you have an s somewhere those s can be propagated to one side.

So send all s to the left side and we will get sr raise to minus i and so on, so once all the s's has been accumulated at one end we will have some expression of the form, s raise to k r raise to j or j prime and s raise to k we can simplify it to either identity or s because s square is doing 2 flips that is equal to doing nothing or the identity operation, so by using these rules all the expression that could come out of multiplying r and s is we have the complete multiplication table for r and s.

So sr raise to i, sr raise to j in particular would be r minus i ss r raise to j that is going to be s square as identity so minus i plus j, okay. All these additions you can think of as been carried out in mod n, okay.

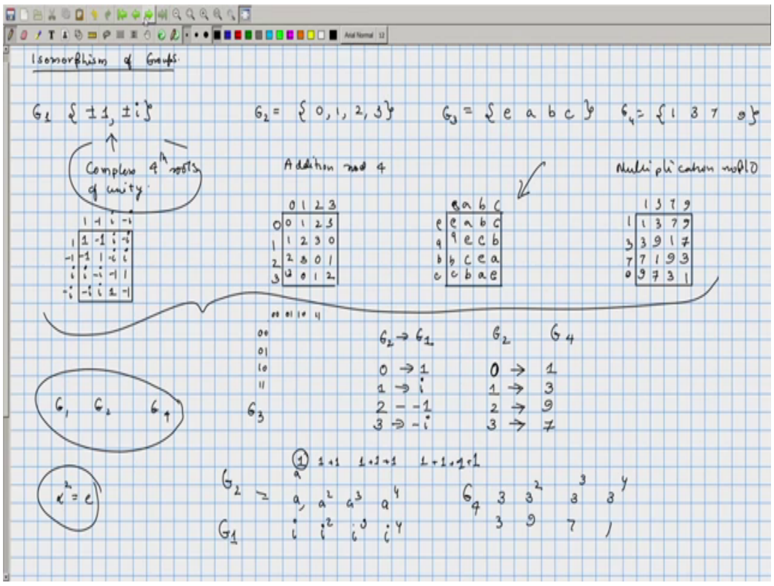
(Refer Slide Time: 32:18)



So what this means is, the entire dihedral group can be described as consisting of basically r and s and their combinations, so we will say that rs is a generator for D 2n okay, with the restriction that r raise to n is equal to identity, s square is equal to identity and rs is equal to s r inverse and see that this is going to be a non-commutative group, so here if you look at the group, the group is of order 2n, there are 2n elements and look if you look at the element r its order, so order we are using in multiple ways.

When we say order of a group that means the total number of elements and when we say order of a particular element, so for example the order of r is equal to n, the order of s is equal to 2, so now that we have seen many examples of groups we will move on to learn more about the abstract concept of group.

(Refer Slide Time: 33:46)



We will introduce the notion of isomorphism of groups, so let me describe 4 different groups and you can think whether these groups are same in certain sense. The first collection of elements is subset of complex numbers namely plus or minus 1 and plus or minus I, okay so these are the complex roots of unity, so or fourth roots of unity, plus or minus 1 and plus or minus i, okay these are elements as it you can multiply that.

So these 4 elements the complex multiplication is well-defined and you can combine them and you can verify that these form a group, let me call this as G1, okay. If I write the multiplication table for this that will look something like this, here one is the element which serves as the identity 1, minus 1, i, minus i these are the 4 elements and one will multiply leave the elements invariant minus 1 square is 1, i square is minus 1, minus i square is also minus 1.

And we can fill up this table, okay my second group here is elements consisting of 0, 1, 2, 3 and I am considering addition mod 4, so again the elements at 0, 1, 2, 3 the identity in this case would be 0, 1 plus 1would be 2, 1 plus 2 would be 3, 1 plus 3 will be 4 which mod 4 is 0, so both these are groups with 4 elements. Another group is the familiar group that we have introduced and the we have started with consisting of 4 elements e, a, b and c and their multiplication was given.

So we said e is the identity and 2 elements when they, I mean any element which multiplied by itself gives the identity and two elements, two different elements when they are combined they give the third element, so b times a is c, b times c is a, a times b is c, a times c is b, c and a combines to give b, c and b combines to give a.

The 4th group that we will consider is elements 1, 3, 7 and 9 and the operations that we are considering here is multiplication mod 10. Okay so 1, 3, 7 and 9 are going to show as the elements and 1 is going to play the role of identity 1, 3, 7, 9, 3 into 3 is 9, 3 into 7 is 21 mod 10 that is going to be 1, 3 into 9 is 27 that is going to be giving 7, 7 to 3 is 1, 7 to 7 is 49 that is going to be 9 mod 10, 9 into 7 is 63 that is 3 mod 10, so we can fill up this table.

Okay so these are all 4 elements groups but are they really different groups? Or some of them just I mean instead of, see if here if I had instead of writing 0, 1, 2 and 3 if I had written let us say, if I named them as, if I had written this entire thing in binary so 00, 01, 10, 11, 00, 01, 10, 11 and filled up this table they are exactly the same in a certain sense, it is just that the names are different, so up in renaming these 2 groups are the same, here also although the numbers are, mean whatever is used to write down those groups looks different or they are just renaming of each other.

So can we find the renaming of one of these groups and get the other groups okay, or is that not possible, so we will argue that some of these are same up to renaming and certain others are not. So these 3 groups G1, G2 and G3 are nothing but renaming off each other, whereas (sorry) G1, G2 and G4 renaming is of each other whereas G3 is fundamentally different okay and this is what we will say I mean when we are looking at group theory to states this fact we will say that G1, G2 and G4 are isomorphic groups.

Whereas G1 and G3 are non-isomorphic and therefore G2, G3, G4 they are all non-isomorphic groups okay, so how do we see that they are isomorphic? We just have to find renaming. So to show that 2 groups are isomorphic conceptually that is straightforward because all you have to do is find a renaming, okay so some part of the renaming we already have mean 0 acts as the identity, so here 0 should be mapped to 1,okay.

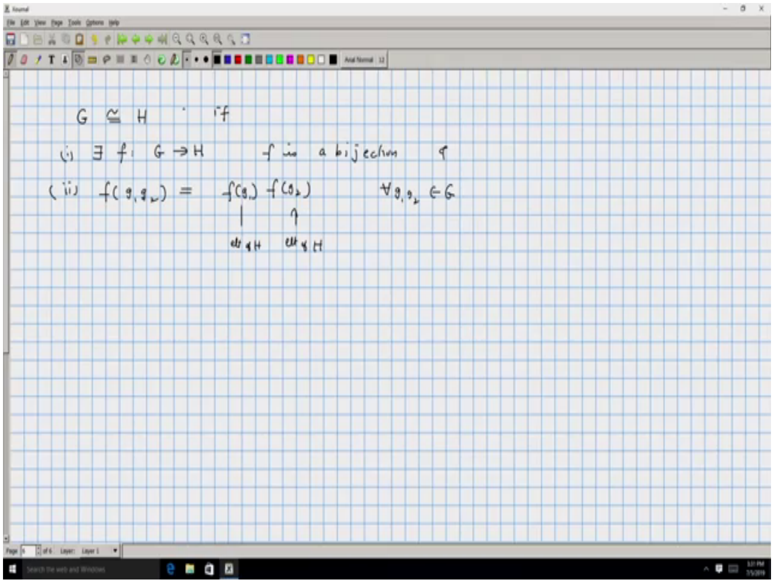
So 0 will map to 1 and 1 we will map to i, 2 we will map to minus 1 and 3 we will map to minus i. If you do this mapping, you can verify that this is an isomorphism from G to G1, okay so G1 and G2 are isomorphic because if you map 0 to 1, 1 to I, 2 to minus 1 and 3 to minus i that will basically make this particular group behave exactly like mod 4 okay and if you want to convert G2 to G4, so 0 will be mapped to 1, 1 will be mapped to 3, 2 will be mapped to 9 and 3 will be mapped to 7.

More easier way of seeing this would be G2 can be viewed as 1, 1 plus 1, 1 plus 1 plus 1 and 1 plus 1 plus 1 plus 1 okay, so this element if we call it as a then G2 is equal to a, a square, a cube, a raise to 4 and if you look at G1 and if we take the element I, the entire collection can be seen as i, i square, i cube, i raise to 4 and if you look at G3 they are nothing but 3, 3 square, 3 cube and 3 raise to 4, 3 square is 9, 3 cube is 27, so 3, 9, 7 and 1 okay, so these are, all these 3 are just another way of representing the cyclic group which contains exactly 4 elements.

Now all that we showed is these 3 are same, how can we say that the 4^{th}, the group G3, here I should have written G4, how do we argue that G3 is very different from G4? So in G3 there is no element which generates the complete collection, it is not a cyclic group because you take any element if you square it so alpha square is equal to identity for every element and therefore it cannot be one of the other 3 groups.

Okay known renaming, if you look at the diagonal, diagonal contains only identity whereas in all the other cases the diagonal contains exactly 2 different numbers, so these are non-isomorphic groups.

(Refer Slide Time: 44:33)



Okay, so formally a group G is isomorphic to a group H if first there should exist a bijection let us call it as f from G to H and further f of G1 G2, so G1 and G2 here are combined using the binary operation in g this should be equal to f of G1 times f of G2.

So f of G1 this is an element of H, f of G2 is an element of H and these when they are combined using the operation that makes H a group, the resultant is equal to f of G1 G2 and this should be true for all G1 G2 belonging to G. If this is the case then we say that f is an isomorphism between G and H and we can say G, if there is an isomorphism we can say that the groups themselves are isomorphic, okay so we will stop this is the end of this lecture, will continue on group theory in the coming lectures.