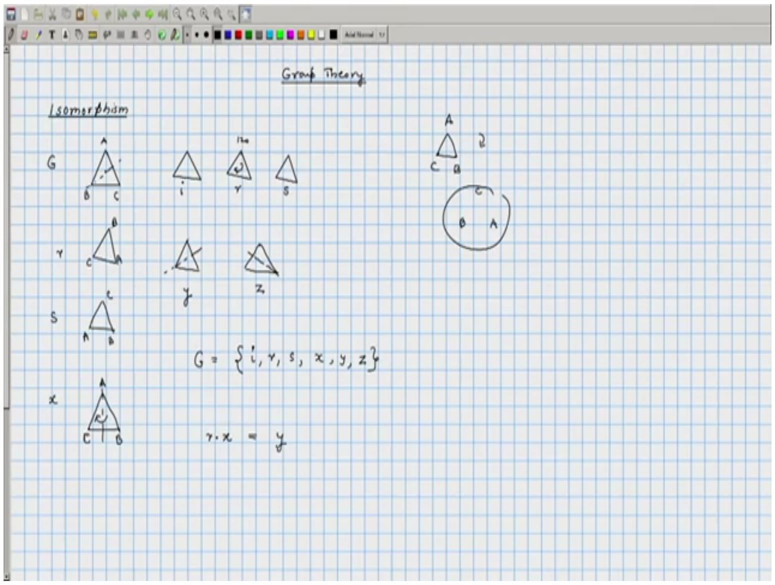
Discrete Mathematics
Professor Sajith Gopalan
Department of Computer Science and Engineering
Indian Institute of Technology, Guwahati
Lecture 40

(Refer Slide Time: 00:40)



Last lecture we were studying isomorphism of groups, we will do one more example of isomorphism. The first group G that we consider will be the symmetries of the equilateral triangle. So consider the equilateral triangle in a plane says the name the word as A, B and C the symmetries of this would be there would be 6 symmetries, 3 corresponding to rotation and 3 corresponding to reflection about a vertex.

Okay so this, so let us name these elements. So first is the identity permutation or which does not do anything, the second would be the rotation by 120 degree about the centre. So suppose we look at the centroid of the equilateral triangle and you consider rotation by 120 degree you will get one particular element of this group.

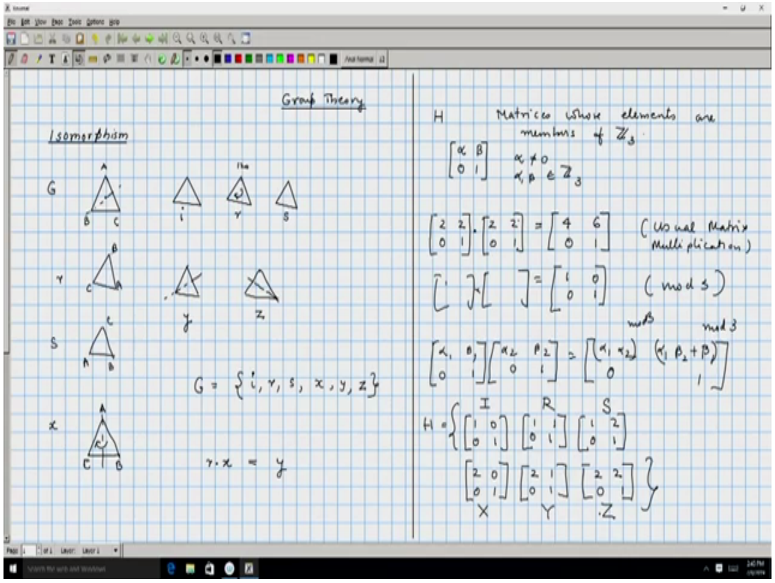
So let us called that as r, okay so that is rotation by 120 degree and then there is a rotation by 240 degree, so r would send vertex as if you look at r this is the permutation that sends A to the position of C and C to B, if you rotate once more let us denote that by S. Than we would get, so and then these are the 3 corresponding rotation and then you can reflect about any one of the axis.

Okay so if you reflect about the vertex about the axis joining A to the centroid, B and C flips okay so let us called that as x, so that is this permutation which keeps A wherever it is and then flips B and C. So C comes here and B comes here, so this is the operation flipping about this particular axis that we will call by x and then there are 2 more other axes.

If you flip about B that we will call as y and if we flip about let say the vertex C what we get is the element z or z. So our group G will basically consist of these 6 elements i, r, s, x, y and z, okay. So these elements when they multiply these dihedral group they multiply in a certain way and you can verify that they do form a group under the operation of compositions of these operations.

Okay for example if you combine r with x okay, so r basically rotates if you start with A B C as labels, so when you say r time x mean you are first applying x, so when you apply x B and C gets flip, so you will end up in the configuration A C B and then you are rotating, so you will reach A B and C. Now this is same as flipping about B, if you have taken the vertex B and if you have flipped about that, what you get is this. So, r x is going to be equal to y. So you can do all the other operations and verify that this do indeed form a group, so this is our first group.

(Refer Slide Time: 05:00)



Group Theory

Isomorphism

$G = \{i, r, s, x, y, z\}$

$r \cdot x = y$

H Matrices whose elements are members of $\mathbb{Z}_3$

$\begin{bmatrix} \alpha & \beta \\ 0 & 1 \end{bmatrix}$ $\alpha \neq 0$, $\alpha, \beta \in \mathbb{Z}_3$

$\begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 0 & 1 \end{bmatrix}$ (Usual Matrix Multiplication)

$\begin{bmatrix} & \\ & \end{bmatrix} \begin{bmatrix} & \\ & \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (mod 3)

$\begin{bmatrix} \alpha_1 & \beta_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha_2 & \beta_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \overset{\text{mod } 3}{(\alpha_1 \alpha_2)} & \overset{\text{mod } 3}{(\alpha_1 \beta_2 + \beta_1)} \\ 0 & 1 \end{bmatrix}$

$H = \{ \underset{}{\overset{I}{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}} \overset{R}{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}} \overset{S}{\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}} \underset{X}{\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}} \underset{Y}{\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}} \underset{Z}{\begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix}} \}$

The second group that we consider which we will denote by H will consist of matrices, okay. So these are matrices, special kind of matrices where the first element, the elements are essentially coming from Z3. Okay so, H basically consist of matrices whose elements are members of Z3 okay, by Z3 we mean numbers from 0 to 2.

So alpha and beta here are going to be members of Z3 and the other 2 elements are fixed 0 and 1 and we have this restriction that alpha is not equal to 0. In particular if you think of these matrices and if you look at their determinant that is going to be non-zero because the determinant is going to be alpha. So H consist of all elements of the form alpha beta 0 1 where alpha is not equal to 0 and alpha beta are elements of Z3, okay.

So now we have specified the matrices and if we look at all these matrices what is the matrix multiplication or the operation that we are interested in here, what is the operation that makes these elements a group? So we will consider the usual matrix multiplication but carried out mod 3. Okay for example, if you take the matrix 2 2 0 1 this is one of the element of H because 2 and 2 belong to Z3 and 2 is not equal to 0.

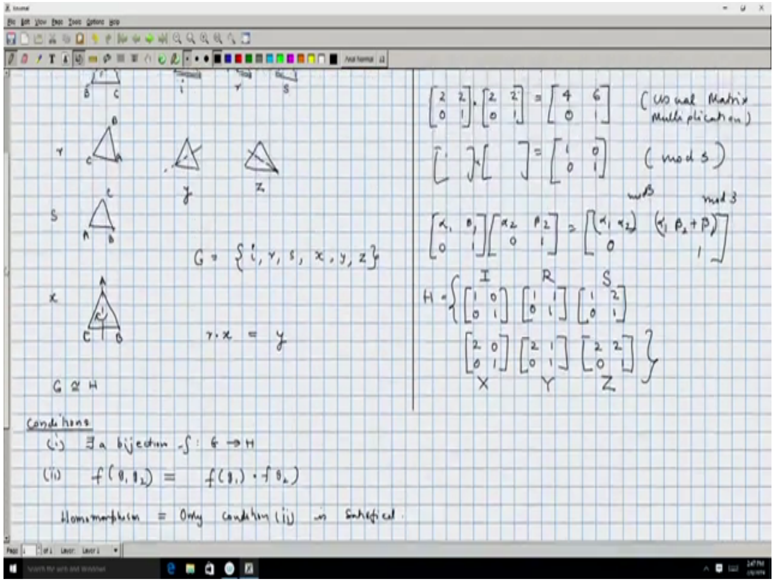
This times let us say the same element 2 2 0 1 this will be equal to you can do the usual matrix multiplication and then you would have got 2 into 2 is 4, okay. But this is not an element of, so this is the usual matrix multiplication but we will do the matrix multiplication mod 3, so then we will get the product as 1, 0, 0, 1, okay. So in particular if you are doing alpha 1, beta 1, 0 1 times alpha 2, beta 2, 0 1 what we will get is and these mod 3 is our final answer, okay.

So clearly this multiplication is a well-defined operation and you can verify that if you took alpha 1 and alpha 2 as not equal to 0 then when you multiply them out you will still get a non-zero element mod 3, okay. So this is our second set H, so H has how many elements? Okay, H also will have 6 elements because alpha there are 2 choices for alpha namely 1 and 2 and beta has 3 choices 0, 1 and 2.

Okay, so the total number of choices is 2 times 3 that is 6. We can write these 6 elements as when alpha is 1 we have 1 0 0 1, 1 1 0 1, 1 2 0 1 and then 2 0 0 1, 2 1 0 1 and 2 2 0 1. So these are 6 elements and now we have and this form up you can check that under the operation that we have defined these 6 elements do form a group.

So now we have 2 groups G and H which both contains 6 elements, so it is easy to get a bijection between them but can we get a bijection which is going to be an isomorphism between the 2 groups? I will give the isomorphism you can check it that the function that I give the bijection that I give is indeed an isomorphism. So 0 maps to let us say capital I, this is capital R, this is capital S, this we call as X, Y and Z check that mapping the small letters to the capital letters indeed is a isomorphism, okay.

(Refer Slide Time: 10:40)



$$\begin{bmatrix}2&2\\0&1\end{bmatrix}\cdot\begin{bmatrix}2&2\\0&1\end{bmatrix}=\begin{bmatrix}4&6\\0&1\end{bmatrix}$$ (Usual Matrix Multiplication)

$$\begin{bmatrix}\ &\ \\\ &\ \end{bmatrix}\begin{bmatrix}\ &\ \\\ &\ \end{bmatrix}=\begin{bmatrix}1&0\\0&1\end{bmatrix}$$ (mod 3)

$$\begin{bmatrix}\alpha_1&\beta_1\\0&1\end{bmatrix}\begin{bmatrix}\alpha_2&\beta_2\\0&1\end{bmatrix}=\begin{bmatrix}\overset{\text{mod } 3}{(\alpha_1\alpha_2)}&\overset{\text{mod } 3}{(\alpha_1\beta_2+\beta_1)}\\0&1\end{bmatrix}$$

$$H=\left\{\underset{}{\overset{I}{\begin{bmatrix}1&0\\0&1\end{bmatrix}}}\ \overset{R}{\begin{bmatrix}1&1\\0&1\end{bmatrix}}\ \overset{S}{\begin{bmatrix}1&2\\0&1\end{bmatrix}}\ \underset{X}{\begin{bmatrix}2&0\\0&1\end{bmatrix}}\ \underset{Y}{\begin{bmatrix}2&1\\0&1\end{bmatrix}}\ \underset{Z}{\begin{bmatrix}2&2\\0&1\end{bmatrix}}\right\}$$

$G = \{i, r, s, x, y, z\}$

$r \cdot x = y$

$G \cong H$

Conditions

(i) $\exists$ a bijection $f : G \to H$

(ii) $f(g_1 g_2) = f(g_1)\cdot f(g_2)$

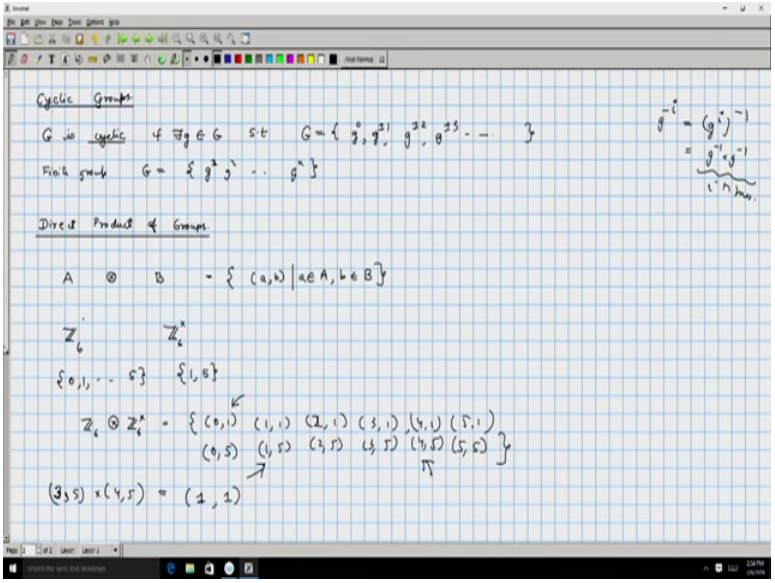
Homomorphism = Only condition (ii) is satisfied.

In order to check that the 2 transfer groups G1 and G2 are isomorphic or G and H are isomorphic we need to check 2 things. The first condition is there exists a bijection say f from G to H and second for this function f, f of G1, G2 that is if you combine G1 and G2 you get another element of G this combination is done as per the operation inside G and if you combine them and look at its image under f that is going to be same as, if you had look at the images of G1 and G2 and then combine it under the operation in H.

So whatever is that result, if these 2 result is same then we say that G and H are isomorphic. So if only one of these conditions is satisfied namely the second condition then we will call this function f which has it property as a homomorphism that means we are unable to find a bijection but there is some function which satisfy condition 2. Then we will say that this is a homomorphism.

So homomorphism is same as only condition 2 is satisfied. Okay so we will study about homomorphism in more detail in the coming lectures. So, now that we have understood what is isomorphism in the earlier examples may be it was straight forward to see that the sets that we have considered were isomorphic here, the groups involved are simple groups the just 6 elements so one can actually try out but it is not obvious to the simple I that these groups are indeed isomorphic under this particular mapping.

(Refer Slide Time: 12:50)



Cyclic Groups

G is cyclic if $\exists g \in G$ s.t. $G = \{ g^0, g^{\pm 1}, g^{\pm 2}, g^{\pm 3} \cdots \}$

Finite group $G = \{ g^1\, g^2 \cdots g^n \}$

$g^{-i} = (g^i)^{-1}$

$= \underbrace{g^{-1} \times g^{-1}}_{i \text{ times}}$

Direct Product of Groups

$A \otimes B = \{ (a,b) \mid a \in A, b \in B \}$

$\mathbb{Z}_6 \qquad \mathbb{Z}_6^*$

$\{0, 1, \cdots 5\} \qquad \{1, 5\}$

$\mathbb{Z}_6 \otimes \mathbb{Z}_6^* = \{ (0,1)\ (1,1)\ (2,1)\ (3,1)\ (4,1)\ (5,1)$
$(0,5)\ (1,5)\ (2,5)\ (3,5)\ (4,5)\ (5,5) \}$

$(3,5) \times (4,5) = (1,1)$

We will learnt some more terms from group theory mentioned about this particular terms cyclic groups. So the definition of cyclic groups says that all elements can be written as powers of some elements. Okay so G is cyclic if there exists small g element of G such that the set G is equal to set g power 0, g power plus-minus 1, g power plus-minus 2 and so on, okay.

So when we write g power minus 1 that would mean the inverse of g power 1 and g power minus i is g power i inverse, okay we could also think of this as same as g power i, g power minus 1 multiplied with itself i times. When as a group all these properties must be true. So a cyclic group is a group where every element can be written in the form of g power i for some integer i, i could be in particular 0, okay.

In case of so this is a general cyclic group, in case of finite group this condition would amount to G being equal to say g power 1, g power 2 and so on up to g power n for some particular n okay when we here n will be the order of the group and it will be the order of the element, okay. So finite group means every element can be generated by just multiplying one element with itself enough number of times. So, in particular if you looked at the roots of unity in the complex roots of unity that is going to be a finite cyclic group of order n.

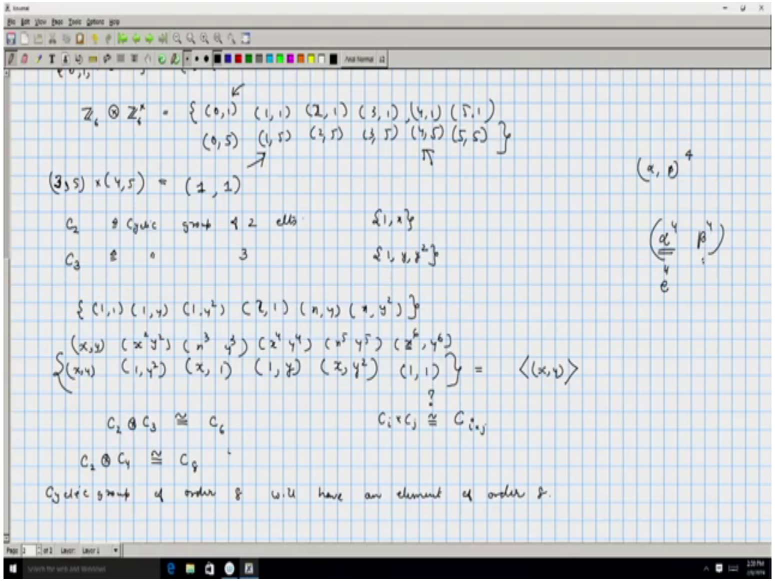
And if you are looking the nth root then you will get the, then you will get a finite of order n. We can verify that up to isomorphism there is only one finite cyclic group or one do not require the condition of finiteness up to isomorphism there is only one cyclic group of any order. Okay the next concept that we will learned is that of direct product of groups. Okay so consider a group A and consider a group B.

Okay we can take the direct product of these 2 groups, we will write it as A multiply A direct product B okay so this consist of say all pairs of the form a, b such that a belongs to capital A and b belong to capital B. If we take these collections of elements, what operation makes them a group? We could multiply the elements coordinate wise and do the operation in the corresponding group, for example if we had taken let say the group that is a Z6, this will consists of element 0, 1 up to 5.

And let us say we consider Z6 star which will consist all element which are relatively prime to 6 namely 1, 2 is gone 3, 4, okay so Z6 direct product, Z6 under multiplication that is going to be consisting of 12 elements namely 01, 11, 121, 31, 41,51 and 05, 15, 25, 35, 45 and 55. So these are the 6 elements. And if you want to multiply 2 elements let us say if you want to multiplied 4,5 with 1,5 okay so 1, 5 multiplied by 4, 5 that is going to be equal to 1 combined with 4.

So 1 and 4 are combined in Z6 so 1 plus 4 that is going to give you 5, if you had taken let us say instead of 1,5 if you had taken 3, 5 and 4, 5, 3 and 4 will combine to give 7 the operation was addition but we have to do it mod 6 and therefore we will get 1. And 5 and 5 will combine to give 5 times 5 is 25 but mod 6 that is going to be 1. Okay so that gives you identity, not identity that gives 1, 1. The identity of this particular group will in fact be 0, 1. So this is defined as the direct product of groups.

(Refer Slide Time: 18:38)



$\mathbb{Z}_6 \otimes \mathbb{Z}_6^* = \{ (0,1)\ (1,1)\ (2,1)\ (3,1)\ (4,1)\ (5,1)$
$(0,5)\ (1,5)\ (2,5)\ (3,5)\ (4,5)\ (5,5) \}$

$(3,5) \times (4,5) = (1,1)$

C_2 = Cyclic group of 2 elts $\{1, x\}$

C_3 = " 3 $\{1, y, y^2\}$

$\{ (1,1)\ (1,y)\ (1,y^2)\ (x,1)\ (x,y)\ (x,y^2) \}$

$(x,y)\ (x^2 y^2)\ (x^3\ y^3)\ (x^4\ y^4)\ (x^5\ y^5)\ (x^6, y^6)$

$\{(x,y)\ (1,y^2)\ (x,1)\ (1,y)\ (x,y^2)\ (1,1)\} = \langle (x,y) \rangle$

$C_2 \otimes C_3 \cong C_6$ $\qquad C_i \times C_j \overset{?}{\cong} C_{i \cdot j}$

$C_2 \otimes C_4 \cong C_8$

Cyclic group of order 8 will have an element of order 8.

$(\alpha, \beta)^4$

$(\alpha^4\ \beta^4)$

$\alpha^4 = e$

Let us look at some simply direct products. If you take let us say C2, okay by C2 we mean the cyclic group of order n of 2 elements, we can write this as 1, x and let us say C3 which is a cyclic group of order 3 and we can refer to the elements as 1 y and y square. Okay now, if you take the direct product of this 2, what we will get is a set consisting of 1 1, 1 y, 1 y square x 1, x y, x y square these are the 6 elements.

And you can check that if you look at elements x y and its powers, so x y powers lets write it down that is going to be x y multiplied with x y so you will get x square y square as a first element, x cube y cube, x raise to 4, y raise to 4, x raise to 5, y raise to 5, x raise to 6, y raise to 6 and so on. There might be other elements but if you look at x raise to 6 that is going to be identity because x square is identity and y raise to 6 is going to be identity because y cube is identity, okay.

So that is, so we do not have to continue further ahead. But are we sure that these 5 elements are all distinct? Now x y is same as x y this one element is present, x square is going to be identity so this is going to be 1 y square. And x cube is just x 1 and x raise to 4, y raise to 4 is 1 y because y cube was 1 and this is x, y square, okay.

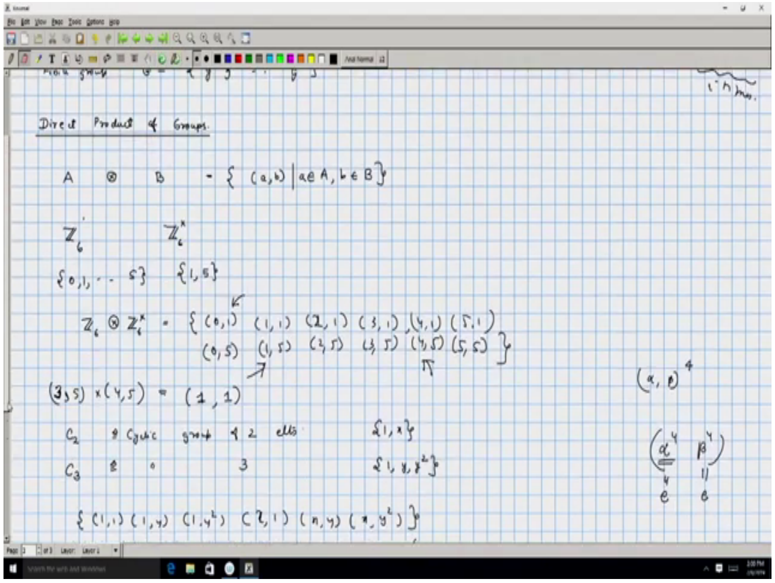
So note that this collection instead of e-e we will write it as 1 1 this is a group with 6 elements, 6 distinct elements and therefore if you look at x y and look at the set generated by x y that means considering all the power of x y we get the complete collection and therefore C2 times C3 the direct product is isomorphic to the cyclic group with 6 elements.

So we can wonder whether this is a general rule that mean if you take the group of order i and order j the cyclic group of these orders and then multiplied you get the cyclic group of order i times j that is not always the case we will see by an example and you can try to answer the question as to. When will these groups be isomorphic? That is when will C i times C j be isomorphic to C i times j okay, when will this what is a necessary and sufficient conditions for such a thing happening.

Now first we will see why this is not always the case because if you take C2 and C4 and we can ask this question, is it isomorphic to C8? Immediately see that is not going to be the case because the cyclic group of order 8 will have an element of order 8. So it is going to be one element which generates the entire thing whereas if you take any element in C2 times C4, okay so let us call that as alpha, beta okay.

Now if you raise it to the fourth power alpha beta power 4 what you will get is alpha raise to 4 beta raise to 4. Now alpha is from C2, so alpha raise to 4 is going to be the identity of C2 and beta raise to 4 that is from a group of size 4 and that is going to be equal to identity okay any element you can check that any element in C4 if you multiplied with itself or perform the group operation 4 times then you are going to get identity and therefore, there is not going to be any element of order 8 and therefore these are going to be different.

(Refer Slide Time: 23:33)



Direct Product of Groups.

$A \otimes B = \{ (a,b) \mid a \in A, b \in B \}$

$\mathbb{Z}_6$ $\mathbb{Z}_6^*$

$\{0,1, \ldots 5\}$ $\{1,5\}$

$\mathbb{Z}_6 \otimes \mathbb{Z}_6^* = \{ (0,1)\ (1,1)\ (2,1)\ (3,1)\ (4,1)\ (5,1)$
$(0,5)\ (1,5)\ (2,5)\ (3,5)\ (4,5)\ (5,5) \}$

$(3,5) \times (4,5) = (1,1)$

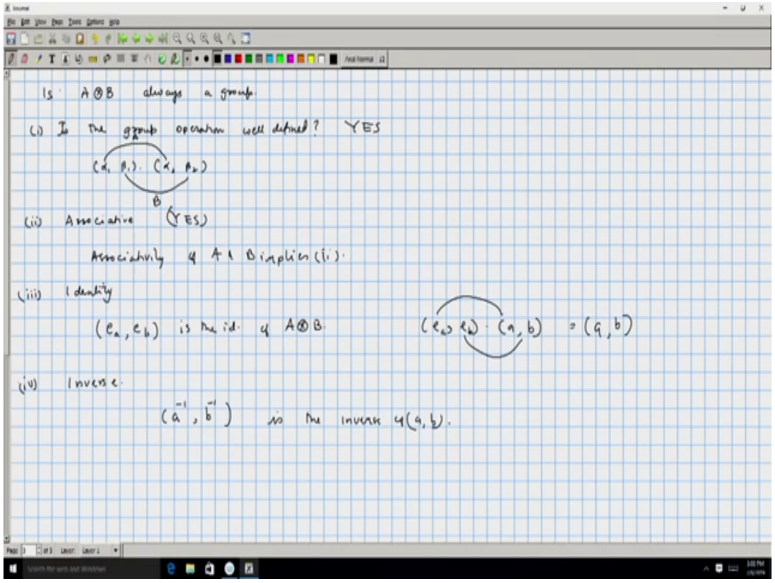
$(a,b)^4$

C_2 : Cyclic group of 2 elts $\{1, x\}$

C_3 : " 3 $\{1, y, y^2\}$

$(\alpha^4\ \beta^4)$, e e

$\{ (1,1)\ (1,y)\ (1,y^2)\ (x,1)\ (x,y)\ (x,y^2) \}$



Is $A \otimes B$ always a group.

(i) Is the group operation well defined? YES

$(\alpha_1\ \beta_1) \cdot (\alpha_2\ \beta_2)$ B

(ii) Associative (YES)

Associativity of A & B implies (ii).

(iii) Identity

(e_a, e_b) is the id. of $A \otimes B$. $(e_a, e_b) \cdot (a,b) = (a,b)$

(iv) Inverse.

(a^{-1}, b^{-1}) is the inverse of (a,b).

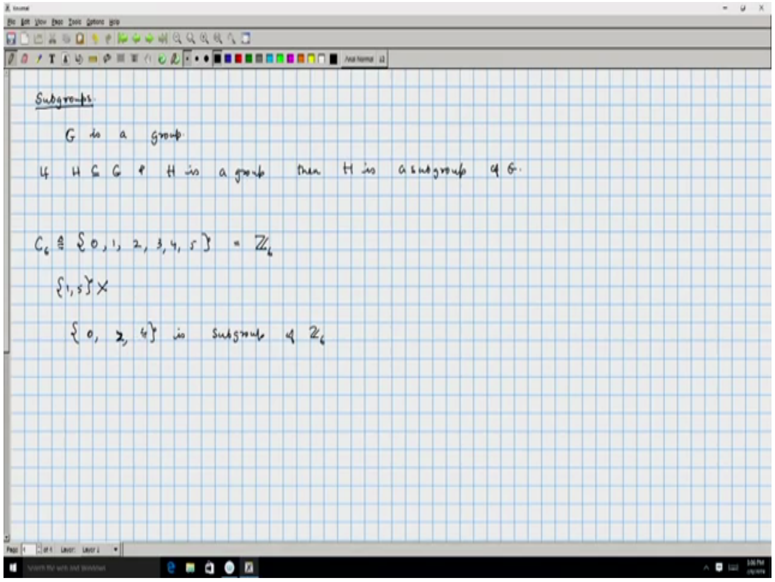
The next concept that we will see is that of sub groups. So, one thing that we did not expressively mention was if we define the direct product of groups in this particular manner why is it that it will always be a group. So, this is the question that you can bother is A direct product B always a group we have to check 4 condition first is the group operation well defined, okay clearly it is because you take 2 elements let us say alpha 1, beta 1 and multiply it with alpha 2 beta 2, alpha 1 and alpha 2 can be combined in A, beta 1 and beta 2 can be combined in B.

And resultant element is clearly an element that is set that we have described and since now the operation is well defined we can check if it is associative, this also yes because that follows from the associativity of A and B because the underlying groups A and B are associative you can verify that it translate into associativity of A times B, A direct product B.

The third is the identity property. So let us say ea is the identity of A and eb is the identity of B this will act as the identity of A direct product B this is easy to check for a conditions of identity ea, eb multiplied with any element A B, this is going to be ea combine with A and eb combine with B, by ea by the property of ea being be identity of A this will give you A and eb times B similarly will give you B.

Okay so, that can be easily verified and similarly you can verify inverse as well, if you have an element a, b, its inverse in going to be a inverse, b inverse, so a inverse, b inverse is the inverse of a, b, okay. So direct product will always be a group and lot of properties from the group would translate into the properties of the direct product, for example if you take a billion groups in B their product will also remain a billion. That is commutative it is preserved under this but that is not true for all properties, if a and b are cyclic that does not necessarily mean that A times B is going to be cyclic.

(Refer Slide Time: 26:40)



Subgroups.

G is a group.

If $H \subseteq G$ & H is a group then H is a subgroup of G.

$C_6 \triangleq \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6$

$\{1, 5\} \times$

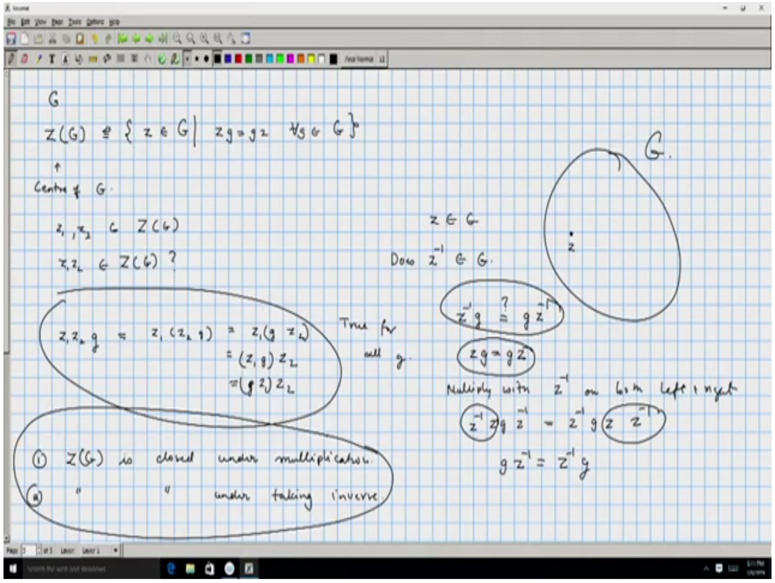
$\{0, 2, 4\}$ is subgroup of $\mathbb{Z}_6$

The next concept that we will learnt is that of subgroups, okay the notions is very simple, so if you have a group G, when we say G is a group we mean that G is the name of the set and there is an operation define on that which makes it a group. So if H is a subset of G and H is a group with the operation now being restricted, if so we do not take these elements and look at a completely different operation but we look at the same operation on G but restricted to the elements of H.

So under that if H is a group then H is subgroup, this is a definition of a subgroup, okay. So, for example if you consider this 0, 1, 2, 3, 4, 5 okay this is C6, the cyclic group of order 6 and we can also think of this as Z6, its additive group, this is a group, now if you look at let us say elements 1 and 5 under mod 6 multiplication if you took 1, 5 that is a subset of the group that you have considered by the operation that you are considering as changed.

So this will not be called as a subgroup of set 6, whereas if you take element 0, 2 and 4 this is a subgroup of Z6, okay you are considering just the even elements of Z6 and under the same operation that is mod 6 addition if you look at these elements they from a subgroup, but 0 acting as a identity and 2 inverse would be 4 and 4 inverse will be 2.

(Refer Slide Time: 28:51)



G

$Z(G) \overset{\text{def}}{=} \{ z \in G \mid zg = gz \ \forall g \in G \}$

↑
Centre of G.

$z_1, z_2 \in Z(G)$

$z_1 z_2 \in Z(G)$?

$z_1 z_2 g = z_1 (z_2 g) = z_1 (g z_2)$
$= (z_1 g) z_2$
$= (g z_1) z_2$

True for all g.

① Z(G) is closed under multiplication.
② " " under taking inverse.

$z \in G$

Does $z^{-1} \in G$.

$z^{-1} g \overset{?}{=} g z^{-1}$

$zg = gz$

Multiply with z^{-1} on both left & right

$z^{-1} z g z^{-1} = z^{-1} g z z^{-1}$

$g z^{-1} = z^{-1} g$

So now let us consider an arbitrary group G and lets define what is Z of G, okay. So this is defined as all the elements belonging to G such that z g is equal to g z for all g belong to G. Okay, so we are given a group lets call that as G and we are picking those elements such that they commute with every other element, if you take this collection we will call this collection by a name this is called as the centre of G.

Our first question would be is this non-empty collection, clearly identity is one element which has this property identity times G is equal to G times identity okay. So this is a non-empty collection and if you have let us say 2 elements z1 and z2 which belong to z g what about z1 time z2? So let us look at z1 and z2 times any element this is equal to by associativity you can write it as z1, z2 g and z2g because z2 was an element in the centre this is equal to z1, g z2.

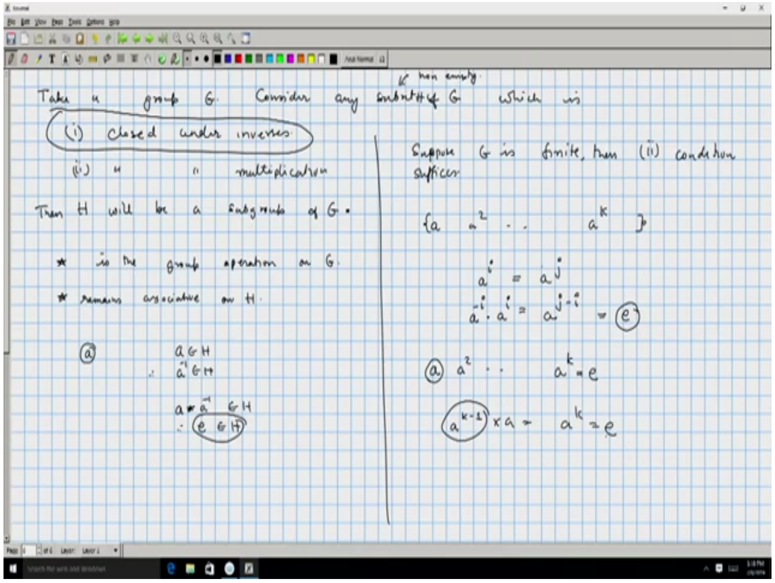
And now again we can apply associativity and write it as z1 g times z2 and that is by z1 being an element of the centre this is equal to g z1 times z2 okay. So z1 z2 g is equal to g z1 z2 for any element g, so whatever we did here was true for all g and therefore if you have 2 elements, their product is also going to belong to z g.

So, if you have some elements this set has the property that it is closed under that operation okay zg is a collection, it is a non-empty collection and now we take any 2 elements z g and you can combine them and the resultant element is still going to be an element. So this is one property that zg has, so we can write this as ZG is closed under multiplication okay let us ask another question. What about Z inverse?

So Z belong to G does Z inverse also belong to G okay now this would mean Z inverse small g is equal to g z inverse this is what we need to prove, that is almost the same statement as the corresponding statement for (Z) z g is equal to g z, so if you just multiply, so consider this equation and multiply with z inverse on both left and right. So both sides if you multiply with z inverse what you get is z inverse z g, z inverse is equal to z inverse g z, z inverse.

Now, these combine to give identity and this also combine to give identity and therefore you get gz inverse is equal to z inverse g and that is what we wanted at the start, that same as this equation. So zg is as a additional property that this is closed under taking inverses. Okay so you have a collection which is a property that you take 2 elements combine them by the operation of the group still the element is going to be there inside this collection and you take any element its inverse is also present. Okay now, any collection which is these 2 properties will in fact be a group, okay so that is if you take G.

(Refer Slide Time: 33:35)



Take a group G. Consider any subset H of G which is
non empty

(i) closed under inverses

(ii) " " multiplication

Then H will be a subgroup of G.

$\star$ is the group operation on G.

$\star$ remains associative on H.

ⓐ $a \in H$

$\therefore a^{-1} \in H$

$a \star a^{-1} \in H$

$\therefore \boxed{e \in H}$

Suppose G is finite, then (ii) condition suffices

$\{a \quad a^2 \quad . . \quad a^k\}$

$a^i = a^j$

$a^{-i} \cdot a^i = a^{j-i} = \boxed{e}$

ⓐ $a^2 \; . . \; a^k = e$

$\boxed{a^{k-1}} \times a = a^k = e$

So take a group G, consider any subset of G which is closed under inverses and is closed under multiplications. So, multiplication here means the group operation, okay. So let us call the subset as H then H will be a sub-group of G, so that is a theorem, we will prove that but if you assume this theorem we now automatically know that z g will in fact be a group.

For any g, finite or infinite does not matter take arbitrary group take any arbitrary group and if you can find the sub-collection of this which is closed under these 2 operations then that will be a subgroup. In particular you could take the entire group and trivially this 2 properties are true and trivially the I mean the entire group is sub-group of itself.

Okay, there are (2) trivial sub-groups of groups namely the full group and the group consisting of only the (())(35:08) element is also a subgroup. Clearly the statement is true for both these cases, it is true for all the other cases as well we will see that in a while. Okay how do we show that H is a subgroup? First of all if you take H, this operation is going to be well define so let say star is the operation, okay. Now star is well defined in H itself because H is closed under the multiplication operation.

And clearly as star was associative it will still remain associative. So star remain associative on H and will identity be present inside this okay so look at an element, so this, so take any group take any subset, so here we mean a non-empty subset. Okay so since it is non-empty there is at least one particular element a and clearly because it is close under inverses, so a belong to H therefore a inverse also belong to H because it close under inverse or since a inverse is there, a star a inverse also belongs to H therefore identity belong to H, okay.

So we have a collection which contains identity it is associative the operation is well defined only additional properties that we need to verify is that very element has an inverse but that something that we have already taken care of in one of our assumptions and therefore H will be subgroup of G or this inverse condition is a special condition that is required only when the group is an infinite group, if it is not infinite suppose you look at a finite group then the only condition that you have to check is that the subset is closed under multiplication.

Why is that so? If we look at any collection, so suppose G is finite then second condition suffices, okay why is that so? Take any element okay if H contain only the identity element then clearly it is a subgroup, so if there was non-identity element present inside it, then call it as a if we look at a, a square so on. At some point a to the power k has to appear, so set this is equal to identity, because otherwise this is going to be any infinite collection.

So, we can just simply argue that since when we are considering a a square and so on some point of time there should be a reputation and le uts say that the first reputation is at i and j, ai is equal to aj but if this was the case, if we look at the inverses of a in the original group lets call that as a raised to minus i, so inverse of a raised to i is a raised to minus i that when multiplied we will get a raised to j minus i is equal to identity, okay.

So, clearly if you consider one element and its powers at some point of time identity is surely going to appear okay, so we can assume that if you consider a a square so for some a raised to k you going to get this is identity and therefore the inverse of a is a raise to k minus 1. Okay because a raise to k minus 1 multiplied by a is a raised to k that is going to be equal to identity. Since this is true for any element a will definitely have an inverse, when this is a when G is a finite group. We will stop here and continue our study of group theory in the next lecture.