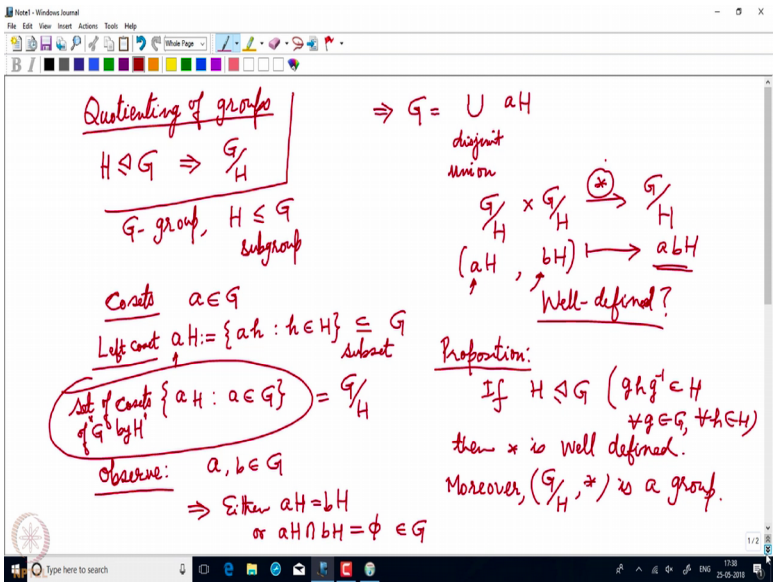
Groups: Motion, Symmetry & Puzzles
Prof. Amit Kulshrestha
Department of Mathematical Sciences
Indian Institute of Science Education and Research, Mohali

Structure of groups
Lecture – 07
Cosets, quotient & homomorphisms

(Refer Slide Time: 00:30)



So, the last lecture, we are talking about quotienting of groups. And I said that when you have a group, which is its normal subgroup of bigger group G, so H is normal subgroup of G, then quotienting makes sense. Today, I will make it bit more precise. So, to start with let us have a group, and any subgroup; A subgroup meaning, a subset of G, which is group in itself under the same operation, which is defined on G.

So, what you can do is you can consider, what are called cosets, so that we take any element in G, and you consider say a H. What is a H by definition? It is a collection of all the elements of the type a h such that h is in H. So, this is a subset of G. So, this is so called left coset, a is coming to the left. We are having group operation, we are multiplying a from the left side, so that is left coset. I know what you do, you consider all left cosets. So, here I am considering a H such that a is in G. So, for two different a in G, so say a 1, and a 2 different. You may actually have same coset a 1 H, a 2 H, it is quite possible.

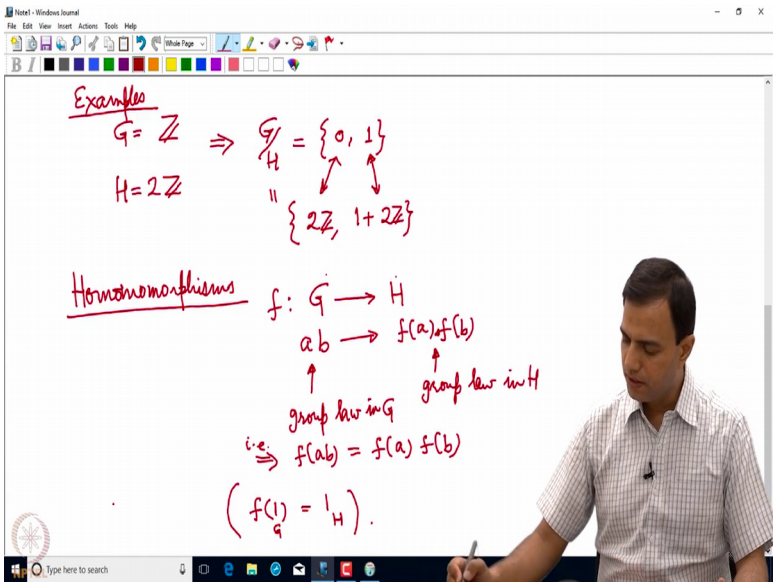
So, you have this collection of cosets. So, this is set of cosets of G by H, so these are cosets. And one has to observe that if I take two element, say a, and b, then either a H is same as b H, or subset a H does not intersect subset b H. So, this intersection is taking place in G, intersection is happening in G, so that means G can be written as union and disjoint union, disjoint union of these courses.

Let us come back to the set of cosets, I will denote it by G mod H it is notation. And on this G mod H, I try to define group operation. How do I do? I just trying to say that if I take one element here, this is a coset, another element, which is here it is a coset, I define it a b H; Then in order to say that all this makes sense. This operation should be well defined, so that is all is a question, is it well defined, because the choice of a, could be something else, choice of b, could be something else. So, choice of a could be something, so that a H is same as a dash H, some other choice right.

Similarly, we could have some b dash H, such that b dash H is same as b h, but b is different from b, b dash is different from b. Then because choice is involved the question of well definedness is certainly there. And it is a proposition that if H is normal, H normal subgroup. I hope you define what normal subgroup is normal subgroup is the one, for which for every choice of G in G, and for every choice of H in H, the conjugation G and G inverse belongs to H.

So, if H is normal, then this operation that I have defined, it is well defined. And in that situation, if you consider set this along with the operation that has been obtained in this fashion, and it is actually a group. So, star, these star operations actually group operation, so that is about quotienting. Quotienting has many applications.

(Refer Slide Time: 07:39)



Let us see some quick examples of quotienting. I have G is equal to Z, integers H is equal to 2 Z, even integers. Then G mod H is just group of two elements. Group of two elements, just write as say 0 1. Why am I writing it as 0 1, here 1 plus 1 is 0, why am I writing like this. Because what are the cosets, cosets would be cosets corresponding to identity, so this is 2 Z, and then 1 plus 2 Z, these are the cosets. And this called coset corresponds to 0, this coset corresponds to 1 is a trivial example of quotienting.

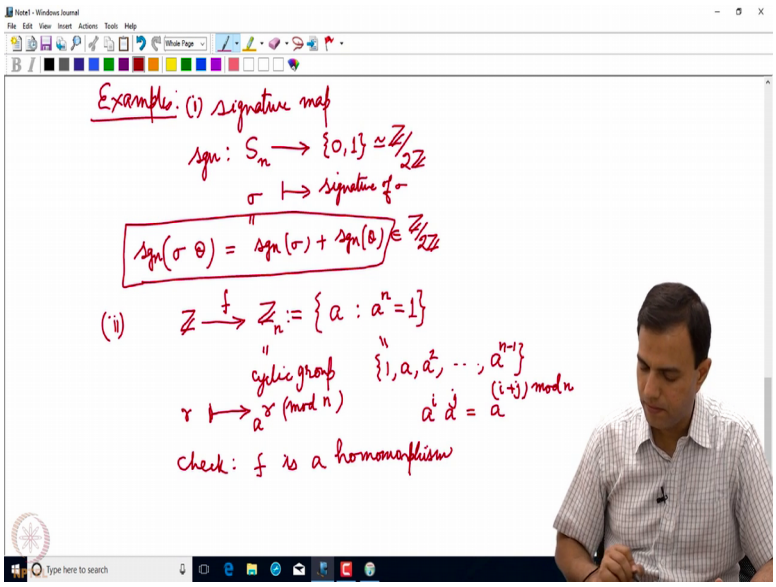
Now, I will discuss some more concepts, remember what is the purpose, purpose to understand Rubik's group, and you solve Rubik's group. Some quotienting will be required there, and some understanding of generators and relations expressing a group, in terms of generators and relations will also be required there.

So, let us see few more things homomorphisms. So, what is the meaning homomorphism of the same type right. So, suppose I have a group G, I have another group H, it is a map between these function from G to H, function f I called homomorphism. If whenever I have two element say a and b here in G, they actually map to the a into b actually maps to f a f b.

What is this? This is the group law in H. What is this? This is group law in G. And so what is being said that is f of a b is same as f of a f of b. Image of the product is product of images. By product what do what do we mean, we mean the group operation, whichever is there in the relevant group H and G. And one of the consequences of this is

that identity of G has to go to identity of H. Why, because you put a and b both to be identity, identity of G, and then you see what happens. So, these maps are called homomorphisms.

(Refer Slide Time: 11:44)



What are the examples? We have seen some of them, you remember signature map. What was that from symmetry group, symmetry group on n letters to say the group 0 1. 0 1 group is what, we have seen it is just Z mod 2 Z odd and even odd plus odd is even.

So, permutation sigma goes to signature of sigma. I hope we recall from previous lectures that for a permutation we can assign, notion of signature. What is that every permutation is a product of transpose, transpose meaning two elements getting swapped. So, if there are odd number of transpose we say the signature is 1 (Refer Time: 12:55) even number of transpose, which are involved in expressing sigma, then you have signature to be 0.

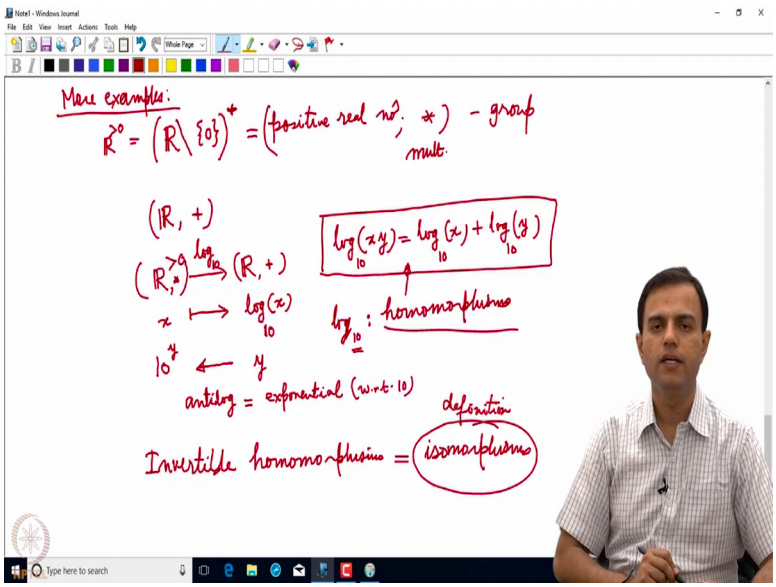
So, if you have sigma n theta, which are two permutations, the signature of them is actually signature of sigma plus signature of theta, and this signature is this addition is actually happening in Z mod 2 Z, so that is one example of homomorphisms. So, you can see this, this is precisely the defining property of homomorphisms.

Another example I can take again quite simple one. I take integers, and then I take cyclic group. What is a cyclic group this one, by definition this is I say in terms of generator

and relations, it is generated by an element a such that a to the power n is 1. So, what are the elements here, elements are 1 identity that is a, a square, and so on up to a to the power n minus 1. So, these n elements are there, and product is formal. So, a to the power i a to the power j, it is simply a to the power i plus j, and this i plus j is happening mod n yeah.

So, I just take say and then you are going to say r I map it to r mod n, so here I would say a to the power r mod n. So, whatever is the remainder after dividing r by n, so that remainder is going to be from 0 to n minus 1, and that as a power of a (Refer Time: 15:23) and that is a homomorphism. So, it is easy to check that let me call this map f, f is a homomorphism.

(Refer Slide Time: 16:08)



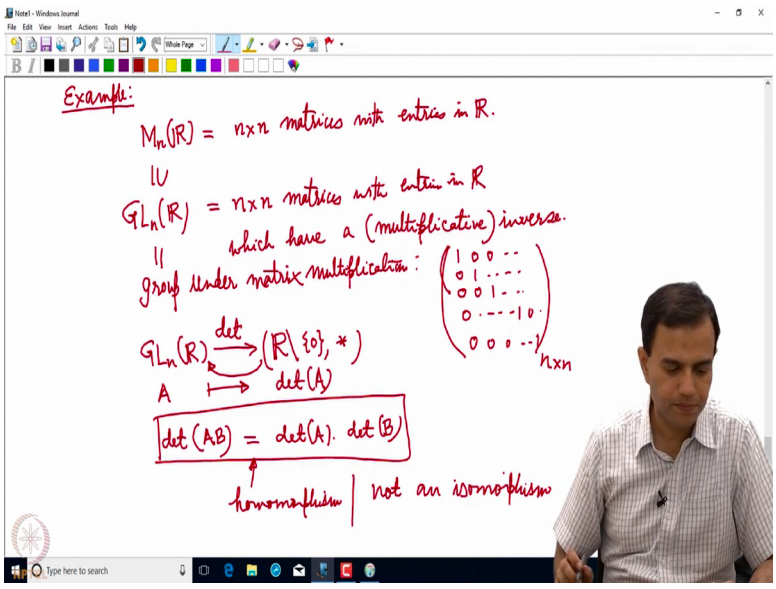
Some more examples of homomorphism, I will mention that is interesting one. You can see the real numbers with 0 removed, and then you take the ones, which are positive, or in other words what you are taking are simply positive real numbers. So, positive real numbers together with usually multiplication form a group.

And then you take real numbers together with addition. So, from positive real numbers, so I would say R strictly positive. So, this is R strictly positive so, R strictly positive. Together with multiplication, just to indicate verification, and then R, the addition. I define this map, when you have known this map for quite long time log to the base let me just say 10 for simplicity. So, a positive real goes to log of x, and the base is 10.

You remember from your school days, at log of x y is same as log of x plus log of y that creation we have seen what was that, it just said that this homomorphism condition, which is satisfied. So, this map log say to the base 10 is a homomorphism, does not matter what base is log to any base is a homomorphism. Here it is multiplication and here it is addition, so that is very interesting example of homomorphism.

And in fact, this homomorphism is invertible. How is that, given any real number, does not matter positive or negative or 0, any given any real number, I can raise it to the power of y. What we called if you remember during this school days, antilog, or it is also call it exponent exponential, exponential with respect to 10. So, for log, we have antilog map, and it combines well, it is a identity. So, such homomorphisms, which are invertible, they are called isomorphism. So, invertible homomorphisms are called isomorphisms definition yeah.

(Refer Slide Time: 20:25)



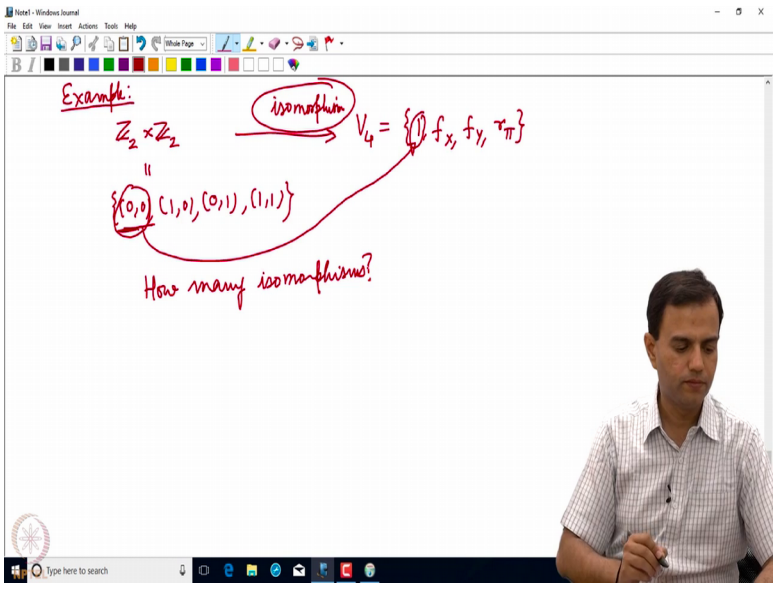
Let us see some more examples of homomorphisms. You consider this set what is that, n by n matrices with real entries with entries in. Is this a group, when you have to tell the operation under addition, it is a group under multiplication it is not a group, because there are so many matrices, which are not invertible under multiplication. So, what I do, I consider those matrices with entries are with entries in R, which have a multiplicative inverse. There that forms a group that forms a group under matrix multiplication. What is

the identity of this group? Like that identity matrix; the matrix, which has all diagonal entries as 1, and all other entries as 0.

So, from this matrix to real numbers with multiplication; so, when I take multiplication, I have to remove 0. So, these are non-zero real numbers. I have to remove 0 with multiplication. Here is a map that we have seen in the school, which is a homomorphism, can you guess it, given any matrix I am going to associate it to scalar determinant. You take a matrix A; you associate to it the determinant of this matrix. And then as you recalled, determinant of A into B is same as determinant of A times, determinant of B. What is it, homomorphism, so determinant is a homomorphism.

Is this may have an isomorphism, that means does there exist a map. In the reverse direction, to which if I compose determinant I get identity, no because there could be two different matrices with the same determinant; So, it is not an isomorphism, because two different matrices of same determinate may exist do exist, so that is not an isomorphism.

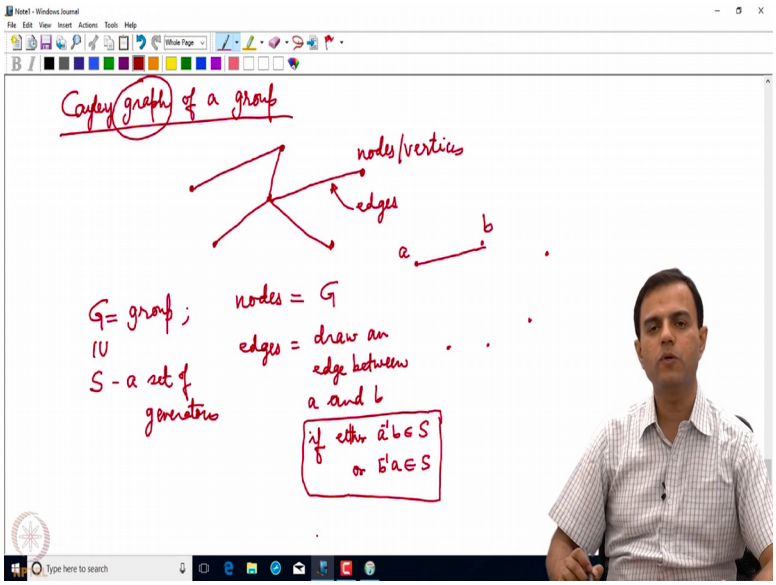
(Refer Slide Time: 25:08)



Let us see one more example. You remember the direct product of groups, what is it, it is 0 0, 1 0, 0 1, 1 1, and then you consider V 4, which I wrote as 1 f x, f y, r pi. When I am writing like this, I want to emphasize that this is group of symmetries of a rectangle. So, one can actually give an isomorphism from here to here, from Z 2 cross Z 2 to V 4. So, of course, (Refer Time: 26:14) is a isomorphism 0 0 has to go to 1. What about the other elements, there are many isomorphisms from Z 2 cross Z 2 to V 4, maybe that is an

assignment question. So, how many isomorphisms are there? So, after this discussion on isomorphisms and the quotienting of groups homomorphisms.

(Refer Slide Time: 27:18)

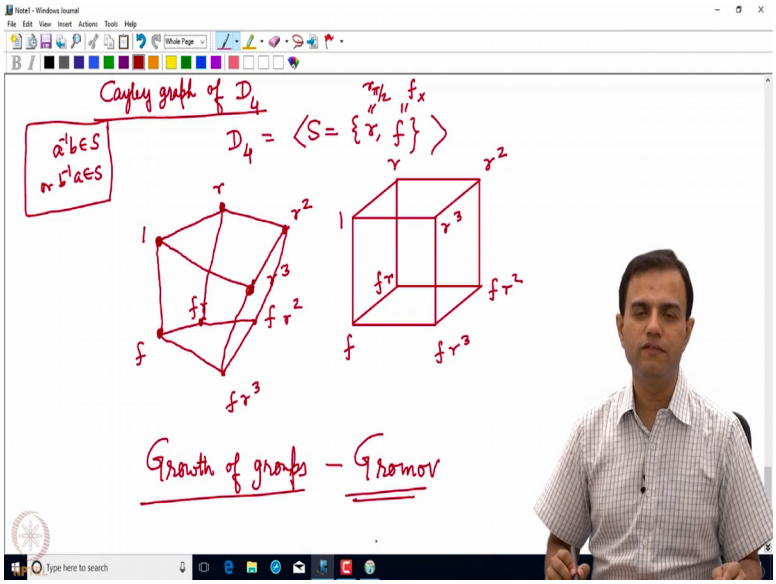


Let me quickly discuss one more concept, which we are going to see in the Rubik's cube case, Cayley graph of a group. So, given a group, and a subset of it, which is generating set, I can think of it is graph, the Cayley graph of the group. So, what kind of graph is this? So, first of all what a graph is, graph is any pictorial representation, where there are several nodes, there are several vertices, and they are connected to each other by a certain rule something. So, there are nodes, these nodes we calls, so call them vertices, and then these are edges.

So, in a Cayley graph, what are the nodes? Nodes are actually all the elements, so I am assuming group is finite. So, all the elements, which are there in the group, I take them as nodes. Nodes are labeled by G and what about edges. So, to define edges, I have to specify that I am writing, I am constructing the Cayley graph with respect to what set of generators, set of generators.

So, what do what we do, suppose these are nodes, these are elements of G. Then here is a element a, here is an element b. I would connect a to b, so edge edges are. So, we drew an edge between a and b, if either a inverse b belongs to the generating set, or b inverse a belongs to the generating set. So, if one of them belongs to the generating set, then you connect the edges.

(Refer Slide Time: 31:01)



Let us see with the example. And your example is a favorite example of say D 4. So, I remember, I hope you also remember that that for D 4, one of the generating sets is r comma f. This is rotation by 90 degree, and this was a (Refer Time: 31:27) about y axis, this is rotation by 90 degree. So, D 4 is generated by this r and f.

And how to draw the Cayley graph so, what are the elements in D, I have identity, I have r, I have r square, I have r cube. So, one will get connected to r, because r times 1 inverse. What are the conditions, the conditions were a inverse b belongs to s, or b inverse a belongs to s, these were the conditions. So, here 1 inverse r belongs to s. So, I am connecting similarly, r belongs to s, r belongs to s, and here also I can make these connections. So, these are four nodes right. And then one is also connected to f.

And then what are other elements, f is there, f r is there as a node, f r square is there as a node f r cube. So, these are nodes. And I am connecting f with f r, because f inverse f r like belongs to s that is r. And similarly, I connect this, I connect this, I connect this, I also connect r and f r, and I also connect, so I am connect connecting r and f r, because f r r inverse, they belongs to the set s.

And similarly, I have to connect r square with f r square, and r cube with f r cube. You realize what we have obtained, it is actually cube. So, the Cayley graph of D 4 is a cube, where if you want I can label like 1, r, r square, r cube, and here f, f r, f r square, f r cube.

So, this is a Cayley graph of D 4. So, in fact, whenever there is permutation, whenever there is a action, which is happening.

When one try to identify what are the basic moves, those basic moves you can think of as generating sets. And then for the whole game, for the whole sequence of permutations, one can create a Cayley graph, and traversing Cayley graph is a fun. There are many other situations, where drawing Cayley graphs is important. One subject area of mathematics is what is called growth of groups, which concerns how these Cayley graphs grow with respect to a set of generators, and what is the effect of choice of set of generators on this growth.

So, if you want, I will give name of the person Michael Gromov, who is one of the pioneers of this area. But, we are not going to study, and growth of groups in this course, we have just interested in various applications of groups. And in particular in some of the situations graph may come, it would be great fun for you to draw a graph of say 15 puzzle, or to draw a graph of Rubik's cube. Can you imagine, how large will the graph of Rubik's cube be, any idea? 1 million, 1 billion, may be more; you will see that we are going to play with Rubik's cube using software, which is called GAP - Groups Algorithms and Programming. You have to watch keep enjoy.

Thank you.