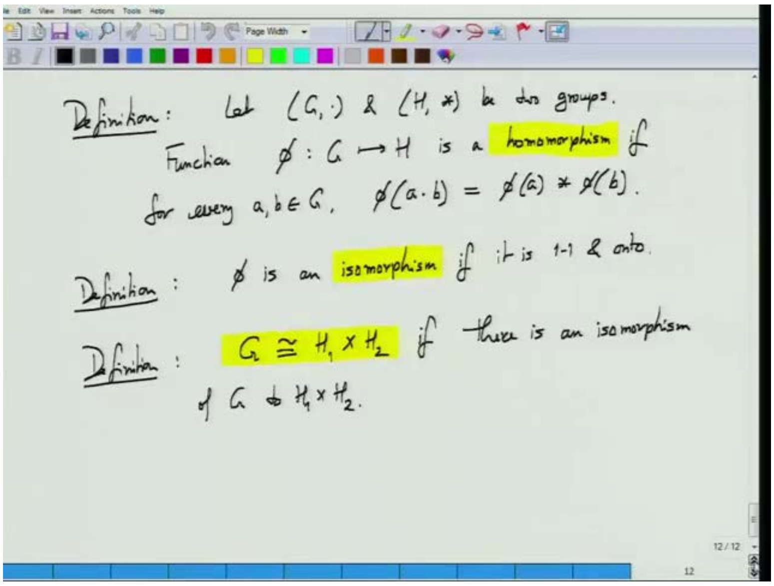
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture - 03
Groups: Isomorphism

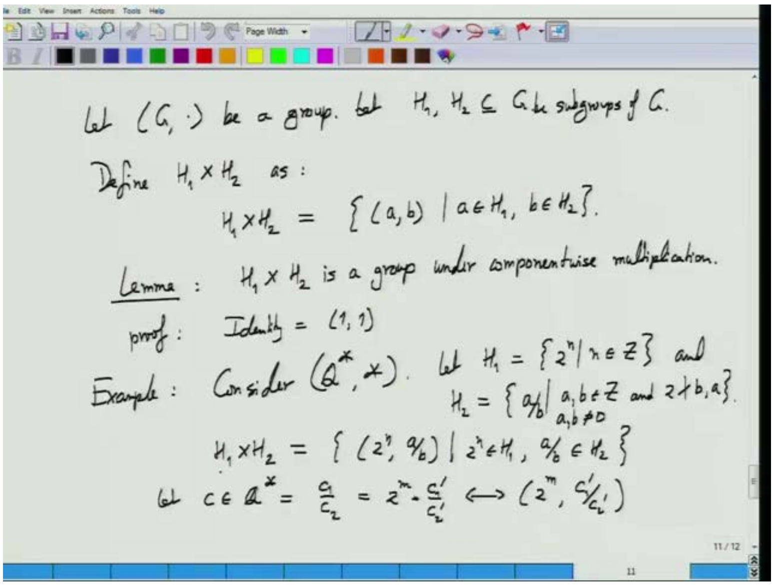
Yesterday, we saw that, we can split some groups into sub groups and write them as a direct product of two groups.

(Refer Slide Time: 00:29)



And, we saw one example, which was q star, which we split as specifically two sub groups; where, the first one was just powers of two; and, the second one was all the rational numbers, where numerator and denominator are odd numbers.

(Refer Slide Time: 00:34)

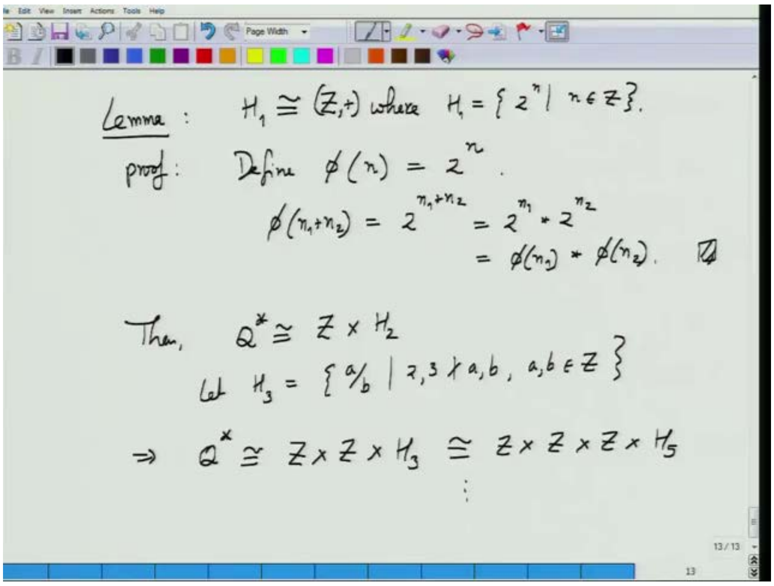


Now, one thing that I would like you to observe, which is also interesting phenomenon is that, if we consider the sub group H 1 here; it is all the powers of two: positive and negative. This is in itself a group under multiplication. Does this group look familiar to you? And, when I say familiar; of course, it is powers of 2 to n. These are very familiar numbers; but, is it a group that you have already encountered before in this course? It is sort of addition, you think so? Why?

Student: (Refer Time: 01:44).

Let us write down this. In the exponent, if you see, of course, there is a 2 with a (Refer Time: 01:53) But, in the exponent, we are just have all integers: positive and negative. And, the multiplication – the group operation, which is multiplication, is the addition operation of numbers in the exponent. So, at least if you think of this group as the operations happening in the exponent, it is simply the group of integers and their addition. But, that is seems (Refer Time: 02:23). So, what is that precisely (Refer Slide: 02:26) We need to have a more precise correspondence between these two groups if we really want to claim something about them. And, thankfully, the notion of isomorphism is just the one that we need.

(Refer Slide Time: 02:45)



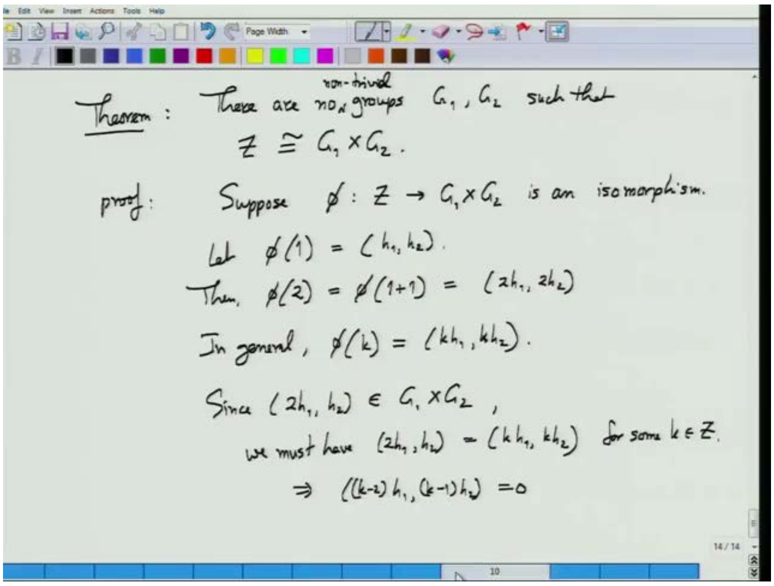
The group which consists of powers of 2 under multiplication is isomorphic to the group of integers and their additions. I should say z plus. Well, for the proof I just need to exhibit in mapping from H 1 to z or conversely from z to H 1, which is one-to-one onto and preserves the group operation. And, that is simple; at least z to H 1 is easier to describe – phi of n equals 2 to the n. This is a one-to-one onto map from z to H 1. Does it preserve the group operation? In the domain, if you add two numbers say n 1 and n 2; so, you consider phi of n 1 plus n 2 is by definition 2 to the n 1 plus n 2; and, that is 2 to the n 1 times 2 to the n 2. This is phi of n 1 times and this is phi of n 2. So, it preserves the group operation. It is one-to-one onto map and that is precisely the definition of an isomorphism of groups.

So, when two groups are isomorphic, we really have the same group really; the only difference is the way the symbols we use to write; that group is different. So, the moment we realize that, H 1 is isomorphic to z, we can go back to where the H 1 came from and we can write Q star as isomorphic to z cross H 2; where, H 2 consists of rational with odd numerator and denominator.

That is already a very interesting fact that, although both are sets of integers, we started from both the groups – Q are not integers, Q star and z they are related groups. But, we found the whole copies of z into Q star. In fact, we can find more copies of z and Q star. If you look at H 2 and take out all powers of 3 from H 2; if we define H 3 as all rational numbers, where numerator and denominator are neither divisible by 2 or by 3; so, this is taking out an all powers of 3. So, I can take out – there is another group, which we have taken out, which is all powers of 3; that is also isomorphic to z for the same reason that all powers of 2 are isomorphic to z. Then we can write Q star as isomorphic to z cross z cross H 3.

Now, we can continue this exercise H 3; we can replace by z cross H 5 – all powers of 5 all (Refer Time: 07:41) We can just continue with this. So, that is an interesting fact that it can write Q star as copies of z multiplied with each other. The next question is how about z itself? Can we write z or we can further divide z into a product of two groups rather? And, the answer to that is no.

(Refer Slide Time: 08:27)



And, I should say just to be very correct, there are no non trivial groups. I can always define G 1 to be z and G 2 to be just the identity element. And then, obviously, it is a product; and, that is really not saying anything interesting. So, no non trivial groups; the non trivial group is a group, which is something more than identity.

And this is also we quite a remarkable theorem, which says that we cannot write z as a product of two sub groups. Proof is very easy actually. And, that proof itself will lead us to something interesting. Let us prove it by contradiction. Suppose there is an isomorphism. Consider where does the number 1 go; the number one will be back by this mapping phi to some element of G 1 cross G 2. So, let us say this is h 1 comma h 2. Then, where does 2 go to?

Student: (Refer Time: 10:33)

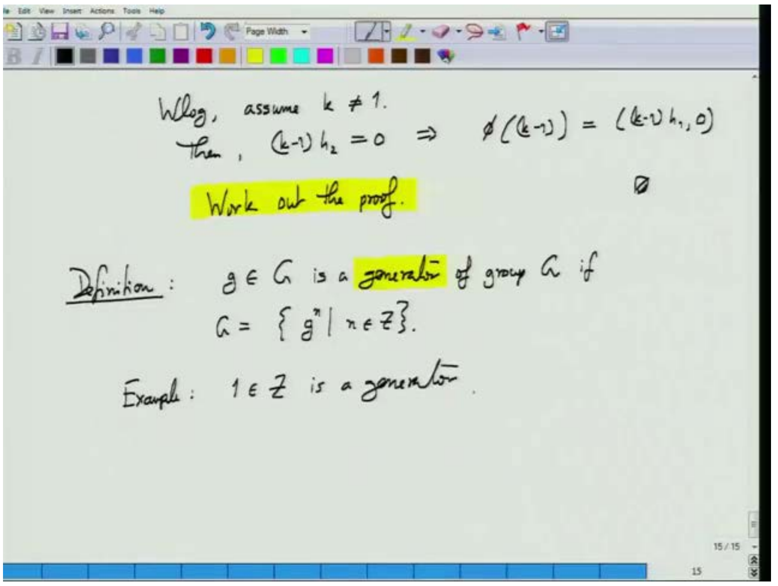
2h – 2 is 1 plus 1. Yes, that is right. And, because phi is an isomorphism, this is same as phi of 1 plus phi of 1. We are writing this group – these two groups also additively here. And, that means, it is 2 h 1, 2 h 2. Here I am taking some liberty with the notation – 2 h 1 is h 1 plus h 2. And, in general, phi of k would be k h 1 comma k h 2. And, this describes the entire range of phi because in the domain now and all, if you look at z, there is just all possible values of k – positive and negative integer and that is mapped to these elements.

Now, phi is an isomorphism. So, the range of phi is entirely G 1 cross G 2. So, that means, in this range, k h 1 comma k h 2. These elements cover the entire G 1 cross G 2; is that true? Is it possible? See phi 1 is h 1 comma h 2; phi 2 is 2 h 1 comma 2 h 2. Now the fact that h 1 h 2 are in G 1 G 2 means that 2 h 1 and 2 h 2 are also obviously there been. Since h 2 is in G 2, 2 h 1 comma h 2 belongs to 2 h 1 comma h 2 is in G 1 cross G 2. So, it must occur in the range of phi. So, 2 h 1 comma h 2 is k h 1 comma k h 2; and then, this is their two group elements. You take this; subtract them; you get k minus 2 h 1 comma k minus 1 h 2 is 0. Is that possible?

Student: (Refer Time: 13:40).

And, that both G 1 and G 2 finite element unless k itself was – well, so, the first thing is k can be either 1 or 2; it cannot be simultaneously both. So, it can only make one of the two components 0 and then it would mean that others.

(Refer Slide Time: 14:09)



So, assume without loss of generality, assume k is not equal to 1. Then, k minus 1 h 2 is 0. This implies that, the element h 2 is very special. You add h 2 to itself a few times, you get 0. So, now, let us see now, what is the simplest way of showing that, we will get a contradiction. Look at phi of k minus 1; that is going to be k minus 1 h 1 comma 0. And, always this helps us. Any suggestions?

Student: (Refer Time: 15:27).

Not necessarily they have.

Student: If we add the see (Refer Time: 15:33) G 1 consists of only h 1.

Multiples of h 1; G 1 considers only multiple of h 1; G 2 consists of only multiples of h 2.

Student: (Refer Time: 15:48)

And after a point h 2 multiples becomes 0. So, that is right. So, G 2 is finite group.

Student: G 1 G 2 (Refer Time: 15:55).

But, is there a contradiction?

Student: If both of them are finite.

If both of them, then it is contradict; but, G 1 – G 2 is finite and G 1 is infinite, then?

Student: One-to-one relationship is (Refer Time: 16:11).

One-to-one relationship is validated?

Student: (Refer Time: 16:15).

Why?

Student: (Refer Time: 16:25) Sir, we have seen G 1 is infinite, G 2 is (Refer Time: 16:50).

G 1 is infinite; G 2 is finite, yes.

Student: (Refer Time: 16:55) h 1 into h 2.

h 1 into h 2?

Student: (Refer Time: 17:00).

2 h 1 comma h 2.

Student: (Refer Time: 17:06).

No, we cannot multiply them. These are G 1, G 2 are two groups when we are just looking at a product of the groups.

Student: (Refer Time: 17:18) h 1 and 2 h 2 are also members of.

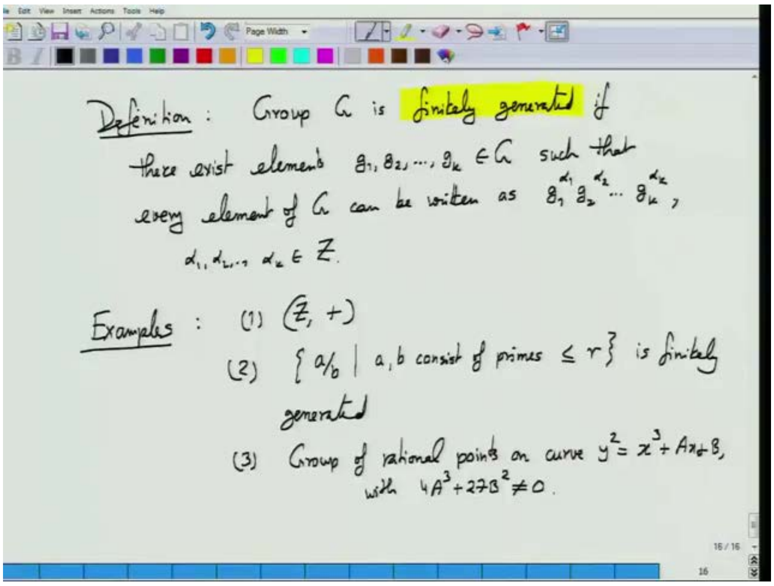
h 1 and 2 h 2 are members of them, right?

Student: (Refer Time: 17:25).

Let us not spend more time on this; work it out. This is a simple assignment problem. I am just losing my way somewhere here; it is a very simple proof. So, that tells us basically that z cannot be divided further into two smaller (Refer Time: 18:07). So, in some sense, z is an individual group – z under addition and Q star is not. So, why is that happening? Why it is that z is individual? The way this proof goes, that should give a hint; we looked at where does 1 go to, because once we know where one goes to, all other elements of z can be decided. So, that leads me to the definition.

So, we say an element small g of every group – capital G is a generator of the group here. The entire group can be written as in terms of small g. So, here I am writing group G as multiplicatively. So, I am writing taking powers of small g in writing g as set of all (Refer Time: 19:56) And, that is the example that we have already seen. 1 in z is a generator. Does Q star have a generator? One number whose with different powers generate the entire Q star. On the other hand, 2 to the n is of course generator, which is 2. So, the existence of generator is a difference, which is making z individual; whereas, Q star is not. And, this observation can now be extended further.

(Refer Slide Time: 20:44)



A more general definition; so, group G is called a finitely generated group. If there exists finitely many elements in g – g 1, g 2 up to g k such that every other element of the group can be written in terms of these elements – g 1 to g k; and, this is the general form of the various elements written in terms of g 1 to g k. Here alpha 1, alpha 2 to alpha k is integers. So, what are finitely generated groups? Are, of course z plus is finitely generated. It has only one generator. This Q star finitely generated.

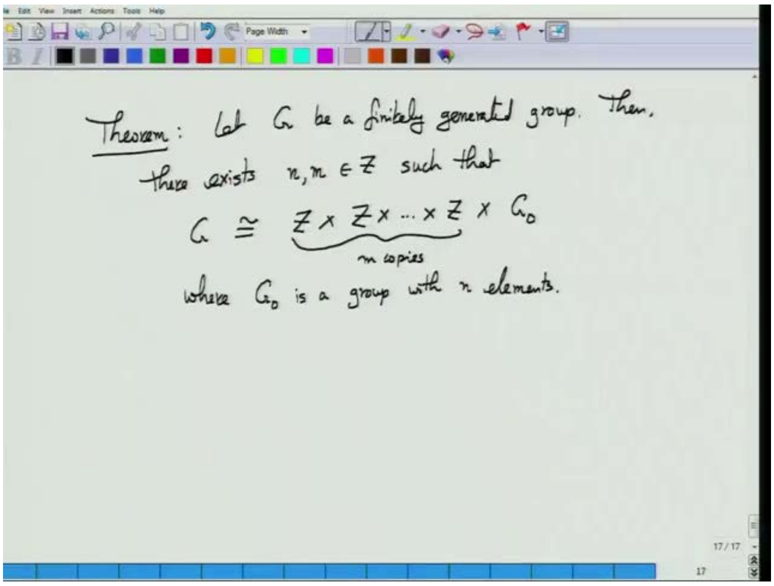
Actually then Q number of generators are in Q star is exactly equal to number of primes and that is infinite. So, the Q star is not finitely generated. The restriction of Q star, where we can say – let us say all a by b, where a, b are – you consider all primes numbers up to some upper bound r. And then, look at all rational numbers a by b; where, a and b only consists of primes up to r. This is finitely generated, because now only you have finitely many prime numbers with which all the numbers are written and that is finitely generated.

Any other example of finitely generated groups you can think of? It is not easy to find out an example of finitely generated group. There are many, but most likely you have not come across that. So, let me give you another example without giving any more details of this example. Maybe later on if we have time, we will come back to this example, look at this cubic curve y square equals x cube plus A x plus B with 4 A cube plus 27 B square is not equal to 0. These are very technical conditions. And, look at all rational points which lie on this curve. When I say rational point, this obvious meaning is that, coordinates of those points must be rational numbers.

Student: Both coordinates?

Both coordinate. And, one can show that there exist infinitely many such points. They form a group under the certain addition operation. And, that group is finitely generated. But, to show this is a very nontrivial exercise and it took very long time for mathematicians to prove it. So, recall that we started with the aim of understanding the structure of groups. And, all these exercise you have done so far expressing it as a product of smaller groups, etcetera is (Refer Time: 26:35) towards it. Now, I am going to give you a big structure theorem, which is very general. It applies to all finitely generated groups. And, it completely describes this structure of these groups.

(Refer Slide Time: 26:53)



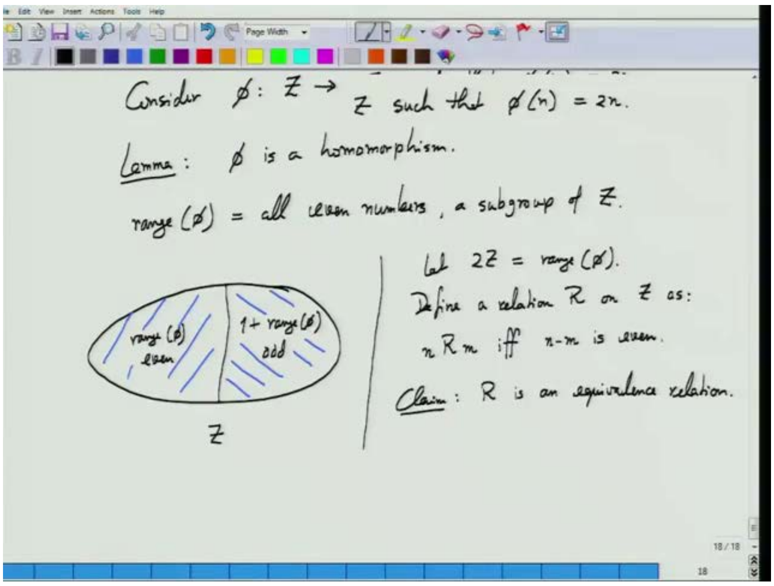
Let G be any finitely generated group. And, in this course, I have already said yesterday, we will discuss commutative groups. So, whenever I say group, I mean commutative groups. This theorem does not hold for non-commutative groups; it is only for commutative groups we are talking. If I talk about non-commutative groups, I will say I am talking about non-commutative groups; otherwise, when I say group, it is a commutative group. So, G is a finitely generated group. Then, there exists two numbers – integers: n and m such that G is isomorphic to z cross z cross up to z – m copies of this cross G naught; where, G naught is a very small group. It is a group; actually, it is with only a finitely many elements, which (Refer Time: 29:05) n elements.

This is describing the structure of any finitely generated group and it is complete description, because z – we have already seen we cannot further split it and the structure of z is very simple. There is just one element 1 that generates this entire group in a very simple way. So, really we cannot have a simpler group than z.

And, there are m copies of z present in it. And then, there is a tiny bit of extra infinite group, which takes out. We will not prove this theorem; I will just give it to you to show that, this exercise or abstraction and then going through all these analysis. Thus have some very interesting consequences that we can prove a structure theorem like this and which is applicable to wide variety of groups coming out of various domains. And, once we have proved this theorem, we do not have to prove it; that is, specifically for the groups, we encounter we already have it.

Now, let us continue further our investigation into groups. This is a nice theorem to know, but this is still not a complete picture of groups, because just look at z. I have said that we cannot split it further, but still z does have sub groups. All even numbers we saw yesterday is a sub group of z. I cannot write unfortunately z as a product of even numbers times some other sub groups (Refer Time: 31:04) But, we would still like to understand the various sub groups of z and how they relate to each other. And, for that, we will use the notion of homomorphism that I have already defined just before defining isomorphism. A homomorphism is a mapping between two groups such that the group operation is present. There is no requirement of the mapping one-one and onto.

(Refer Slide Time: 31:50)



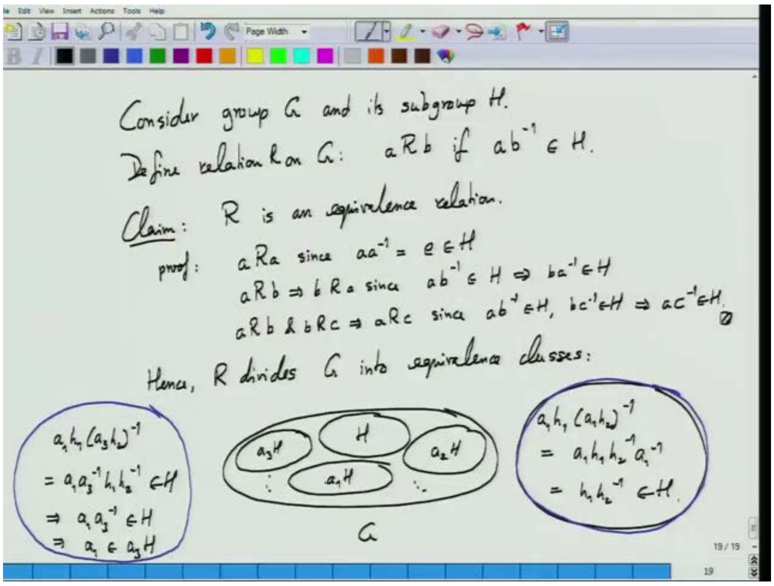
So, consider the following map. (Refer Time: 32:11) multiplication by 2, when I write 2z to represent the subgroup of z, which consists of even numbers. So, phi is a homomorphism. Still we will receive this. The addition of two numbers is mapped to two times the addition of those two numbers, which is just two times one number plus two times the other numbers. The range of phi is all even numbers.

And, that is a subgroup of z. What does it leave out? Phi leaves out all odd numbers. In fact, if you see z, and divided this into even and odd – even numbers and odd numbers; so, this is range of phi; this is not outside the range of phi. However, I can write this as 1 plus range of phi. And, this kind of leads to the following view point that, let us call 2z to be range of phi and define the following relationship.

defining a binary relation on z – set of all integers. And, the relation says n is related to m if and only if n minus m is an even numbe. Do you remember equivalence relations? This relation r is an equivalence relation for all these reasons. A number n is related to itself, because n minus m, which is 0 is an even number. Then, reflexive property n is related to m, which also means m is related to n.

And, transitive property – n 1 is related to n 2; n 2 is related to n 3; that means n 1 minus n 2 is even; n 2 minus n 3 is even - clearly means n 1 minus n 3 is even; so, its relationship is transitive. So, R is an equivalence relation. This equivalence relation as we know, any equivalence relation divides a collection of elements into equivalence classes. So, for this particular relation, we will divide set z into equivalence classes. What are the equivalence classes? Odd numbers and even numbers; these are the just two equivalence classes and those are precisely these. This is one equivalence class; this is other equivalence class. Now, this leads to a more general observation. This we saw in terms of z and sub - a particular subgroup of z. But, now, let us consider in general group and a subgroup of that.

(Refer Slide Time: 37:05)



And, we do the same thing. Just we make that exercise – define an equivalence relation. Or, first define a relation; we will show that there is an equivalence relation. So, a is related to element b. Now, we have to define it with respect to the sub group H. And, in this, remember what we did; we did the subtraction of the two elements. That should be the subgroup. Let us write this group multiplicatively as we would typically do for a general group. So, there we have to say a b inverse is in H; a minus b becomes a b or a (Refer Time: 38:24) b inverse represents the inverse element corresponding to b.

Now, it is straightforward to see that this R is also an equivalence relation for exactly the same reasons – a is related to a; maybe it requires a proof. a related to a since a a inverse, which is the identity. We just write the identity as E and this belongs to the subgroup H. Since H is a subgroup, it has the identity. a related to b implies b related to a since a related to b (Refer Time: 39:34) means a b inverse is in H; H is the subgroup. So, inverse of this element; a b inverse is also in H. What is the inverse of this element? b a inverse. And, a related to b and b related to c implies a related to c since a b inverse in H. b c inverse in H implies the product again; because H is a subgroup, the product is also in the subgroup a c inverse in H. So, it is quite remarkable that, the notion of equivalence relation seem to fit perfectly with the notion of groups.

You see the identity of group is corresponding to the reflexive property. The inverse property corresponds to the symmetry. And, the closure property corresponds to the (Refer Time: 40:47). So, the net result is that, the group G is now divided into equivalence classes. And, these are determined by the subgroup H. You have G G; then, you have H as one equivalence class. The subgroup itself will be a one equivalence class. Then, there will be other side equivalence classes: a 1 H, a 2 H.

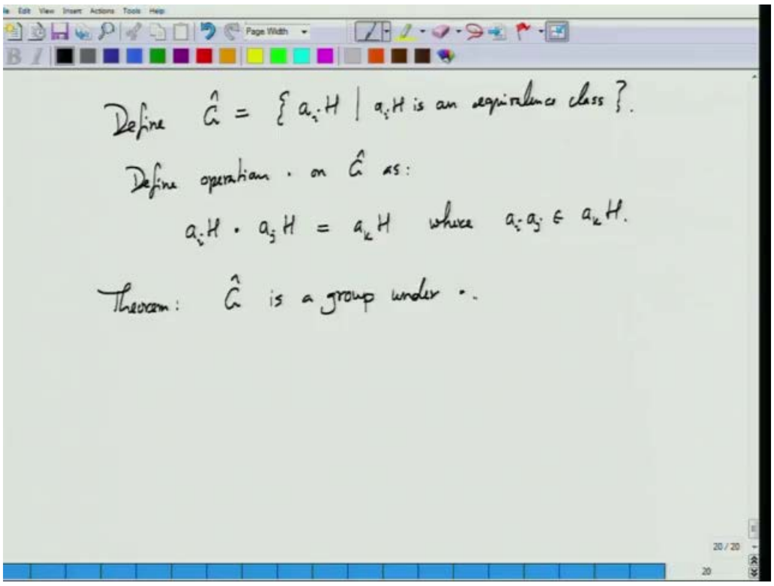
And, I will explain what meaning actually is. a 1 H is simply all elements of the form a 1 times in the element of subgroup H. Why are these? Any two elements related? If you look at a 1 h 1 and a 1 h 2, these are two different elements in this. They must be related to be in the same equivalence class. The relationship properties say a 1 inverse h 1 – h 2 inverse. Why are elements in a 1 h in the same equivalence class? That is the question. So, take two elements in a 1 h; call them a 1 h 1 and a 1 h 2; their inverse – let me just write this again.

What is their inverse? a 1 h 1 a 1 h 2 inverse, this should be in h. So, this is a 1 h 1 h 2 inverse a 1 inverse. This is a commutative group. So, a 1 a 1 inverse takes care of itself. This becomes h 1 h 2 inverse, which is of course in H. So, its commutativity here is essential. If you do not have commutativity, there is a problem. And, this is how we can show them any two. So, clearly all elements in here are in the same equivalence class.

How about two elements across? Can they be in the same equivalence class? That is, this one is one property. Then, let us look at one element from a 1 h and one element from a 3 h. Are they in the same equivalence class? a 1 h 1, a 3 h 2 inverse, this is a 1 a 3 inverse; h 1 h 2 inverse; just rearranging the terms. This is of course in H. So, this is a 1 a 3 inverse. That element will determine the equivalence class it is in. So, let us assume without that, it is in a 1 H. I am saying that all of these – each one of this contained an equivalence class.

The question is can two of them all be contained in one single equivalence class? So, this is one element from here and one element from here. And, suppose this is contained in the same equivalence class, which is that, this is in H; of course, here this is in H. This should be in H. Like that when it is in the same equivalence class. h 1 h 2 inverse is an H. So, this could imply that, a 1 a 3 inverse is in H. This implies that a 1 is in a 3 H. So, these two classes are equal. If a 1 is in a 3 H, then a 1 H is in a 3 H. So, it is the other part of derivation. So, in the end, we have group G is split into disjoint equivalence classes. Each equivalence class being of the form some a 1 times H; now, I will do a little bit of magic.

(Refer Slide Time: 46:22)



Let us collect all the equivalent classes and put them in one set. Call it G hat. And, let us define an operation on G hat. The dot operation on G hat is defined as a i H is one element of G hat; a j H is another element of G hat. Op – they are operated on each other. You get a k H, which is the third element of G hat. This is a k is that, element of G. So, is that, a i a j belongs to a k H.

And, let me state the theorem, which I will prove later. Under this operation, this set of equivalence classes itself is a group. This is, taking some time to observe, because elements of G hat are not elements of G, they are sets of elements of G. And, we are operating on sets of elements through this dot operation in creating such different sets; and, these operation themselves lead – produce group structure on G hat.

We will continue tomorrow.