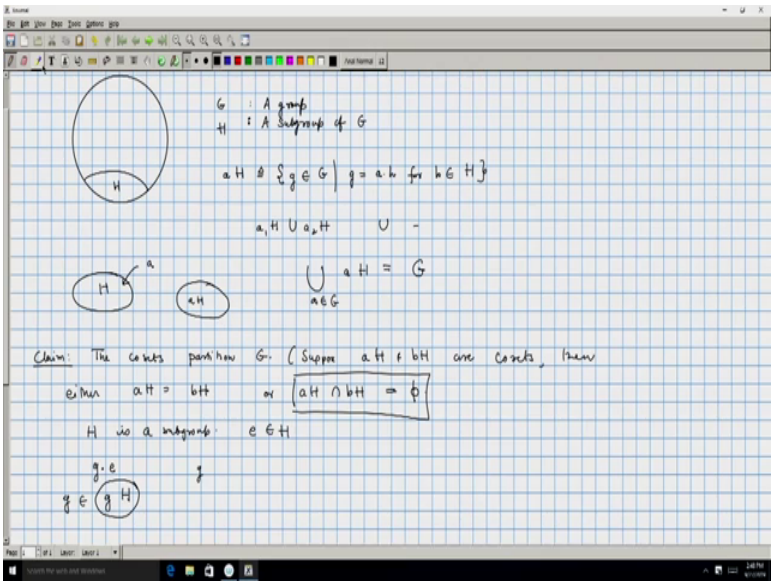
Discrete Mathematics
Professor Sajith Gopalan
Department of Computer Science and Engineering
Indian Institute of Technology, Guwahati
Lecture 41

(Refer Slide Time: 0:32)



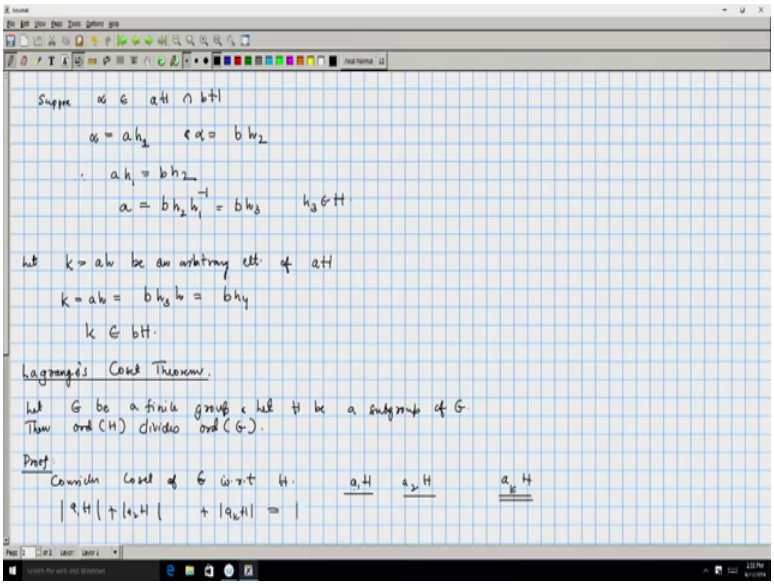
In this lecture we will learn about the cosets and quotient group. So let us consider a group, let us say this is the group G and suppose this is a subgroup H. So let us define what are known as the cosets of G with respect to H. So consider all the elements from aH, okay so aH is defined as all those g belonging to G such that g is equal to a times H for h belonging to capital H, okay. So this is our set H and we went to multiply all the elements in H by a, what we, once we do that we will get another set which we will call as aH.

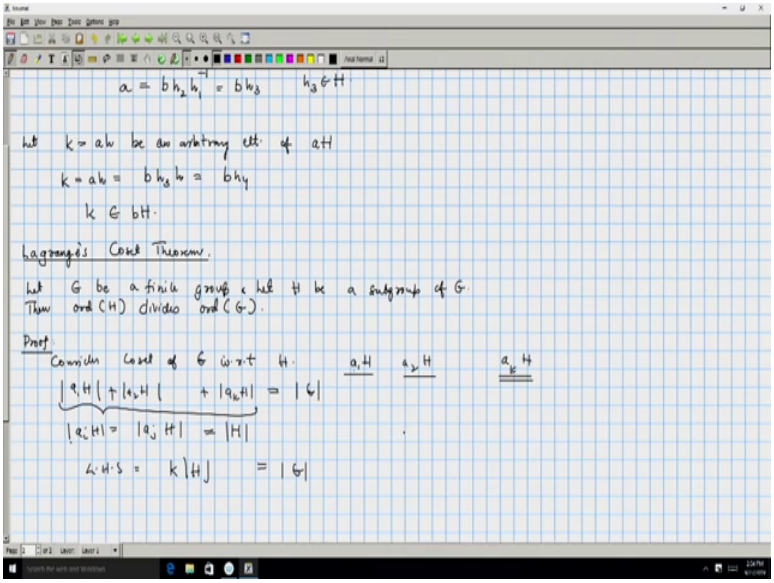
Okay and this is going to be called as a coset. In particular, this is a left coset because we are multiplying on the left. So now if you take an arbitrary group and construct all its left cosets we will get different cosets, let us call them as a1H, a2H and so on. And these collections of cosets is going to, I mean if you take the union of them that is going to be the complete collection. In other words, union over all a belonging to G aH will be equal to the set G.

But what is more interesting is, if you take 2 cosets they either are one and the same or they are disjoints. Okay so this is a claim, the cosets partition G, so if you have, so what this means is suppose aH and bH are cosets then either aH is equal to bH or aH intersection bH is equal to empty. Okay how do we prove this? And if we have this claim, it is easy to see that if you take all the cosets that will and take the union of that you will get the entire set because if you look at H, H is a subgroup, in particular the identity belongs to H, okay.

And if you take 3 times e for any arbitrary g belonging to the group, you are going to generate the element g. So if you consider the coset gH that contains g okay. So the union of gH over all G will certainly exhaust the complete collection of groups. Why is it true that is it either empty or to cosets are the same. So let us assume that the cosets have some non-trivial intersection, if they did not have any intersection, then we are fine because that is just the condition aH intersection bH is empty.

(Refer Slide Time: 4:08)





So suppose, let us say alpha belongs to aH intersection bH, okay so that would mean that alpha is equal to ah1, there exists an h1, an element h1 such that alpha is equal to ah1 and alpha is equal to bh2. And therefore we can say that ah1 is equal to bh2, so ah1 is equal to bh2, therefore a is equal to bh2 h1 inverse. And since h2 and h1 are members of a group, we can say that, this is a subgroup so h2 times h1 inverse will be equals to bh3 for some h3 belonging to H okay.

Let k is equal to ah, be an arbitrary element of aH. We want to show that k will belong to bh and exactly same reasoning will show that any element in bh will also (belonging) belong to ah. So let us first do the, the proof that any element of ah will belong to the set bh okay, so k is equal to

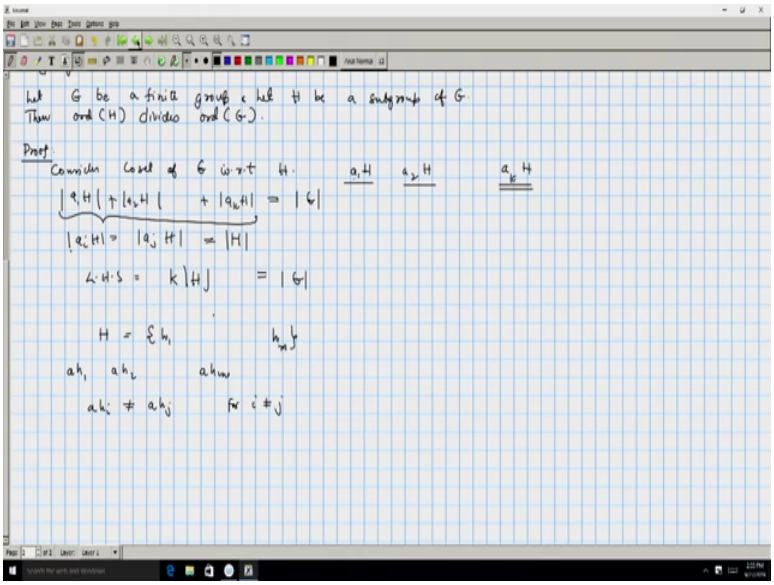
ah, so a can be written as b times h3. So k is equal to ah can be written as b times h3 times and that is equal to b times h4 okay, so this means that k must belong to bh.

So we took an arbitrary element of ah and showed that it belongs to bh, if there is an intersection between ah and bh. And similarly you can show that any arbitrary element of bh must belong to ah, if there was a common element. So that concludes the proof that the cosets are either disjoint or they have a, they are one and the same okay. So now this will help us prove the following theorem known as Lagrange's theorem.

So let G be a finite group and let H be a subgroup of G. So clearly H will also be a finite group, then order of H divides order of G, okay. Why is this true? If you consider so all that one has to do is, consider cosets of G with respect to H, so order of H is number of elements in H and order of G is number of elements in G. So if you consider the cosets with respect to H they are going to be say a1H, a2H and akH okay. So let us say these are the distinct cosets, some of these, mean we have taken all the elements of G, some of the cosets may overlap but here we are just counting the, we are just enumerating the distinct cosets.

Let us say k of them are there, which we called as a1H, a2H and akH okay and these cosets, these collections, partition the collection G okay. So their sizes if you add up, we will get G, so size a1H plus size a2H plus size akH is equal to size of G. But note that every coset is of identical size, size aiH is equal to size ajH, why is this so? This is equal to the size of H. Now if we assume this fact, what we show is what we can immediately conclude is that, the total sum on the left hand side is equal to k into size of H and that is equal to the RHS, which is the size of G. So this would be the proof but all that we may get to see right now is that why are two cosets of identical size.

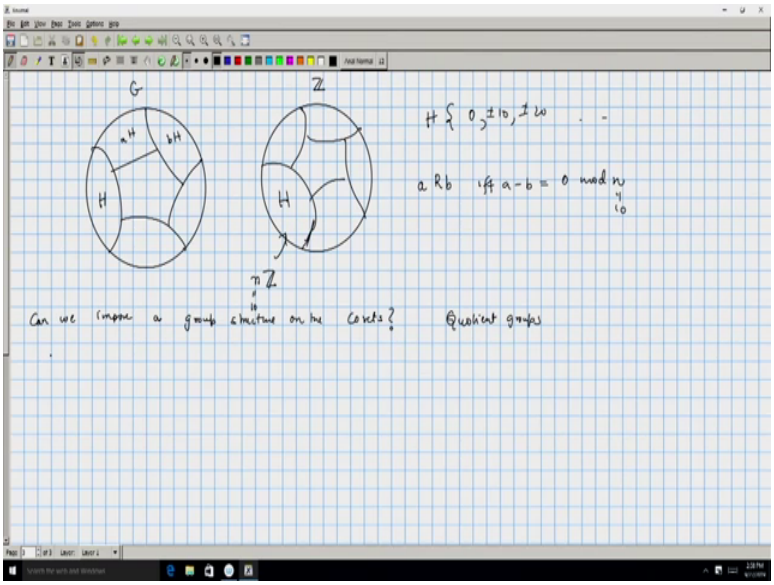
(Refer Slide Time: 8:55)



Now the set H is a finite set and let us say its elements are h1 up to hm okay. Let the sub group of G, its elements be h1 to hn. Now if you look at ah1, ah2 and ahm, these are m elements and they are all distinct because ahi cannot be equal to ahj for I not equal to j. This is because, if we assume ahi is equals ahj, you can multiply both sides of the equation with a inverse and you will get hi equals hj, so this cannot be equal. And therefore there are m elements in ah, where m is a number of elements in the subgroup okay.

So that concludes the proof, the fact that this is the finite group, was used when we said that these partitions has a fixed number of elements and each of this coset is of finite size.

(Refer Slide Time: 10:06)

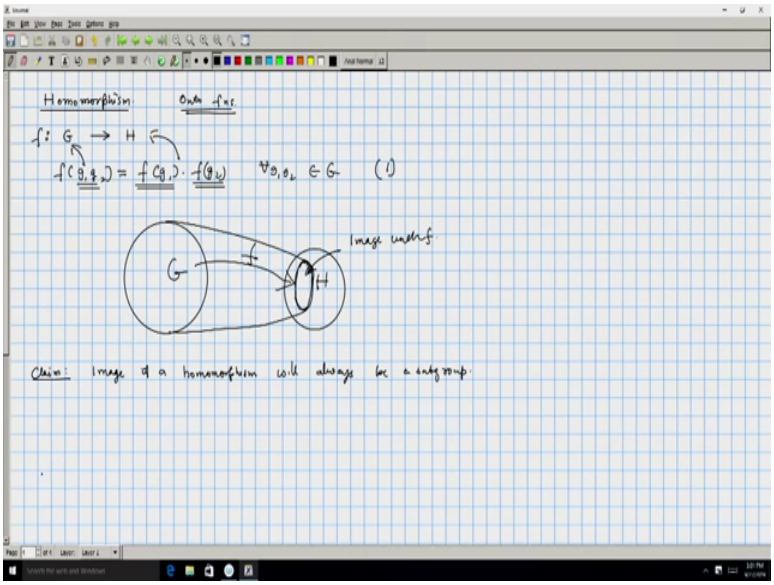


So let us consider a group and these are the cosets corresponding to H, okay so let us say this is aH, bH and so on. If G were the set of integers and let H be the multiples of n, for example if we took n as 10 then H is all those elements of the form 0 plus or minus 10, plus or minus 10 and so on. Now these cosets are basically the equivalence classes, a is related to b if a minus b is equal to 0 mod n, okay here n is 10, okay.

These cosets are precisely those equivalence classes okay and we could, we had seen earlier that we could do arithmetic or we could add and multiply these, these equivalence classes themselves. So the cosets could themselves be added and multiplied. And when can we really do this? Can we impose a group structure on the cosets? Okay so that is the question that we will try to answer. And in some cases we can do that when the (coset), when the group, the underlying subgroup has some nice properties, we can have a group structure on the cosets, okay that is known as a quotient group.

In some sense, you are using the group, the subgroup H to divide the group G into different parts and then we carry out some operations, we define some group structure on the parts obtained.

(Refer Slide Time: 12:27)



So in order to look at these things closely, we will (introduce) we will look closely at the concept of homomorphism. Okay we had seen the notion of isomorphism earlier and homomorphism between G and H, so let us say G is a group and H is another group, a function from G to H is called as homomorphism, if f of g1 g2 is equal to f of g1 times f of g2, g1 g2 is computed in G and f g1 times f g2 that is computed in H.

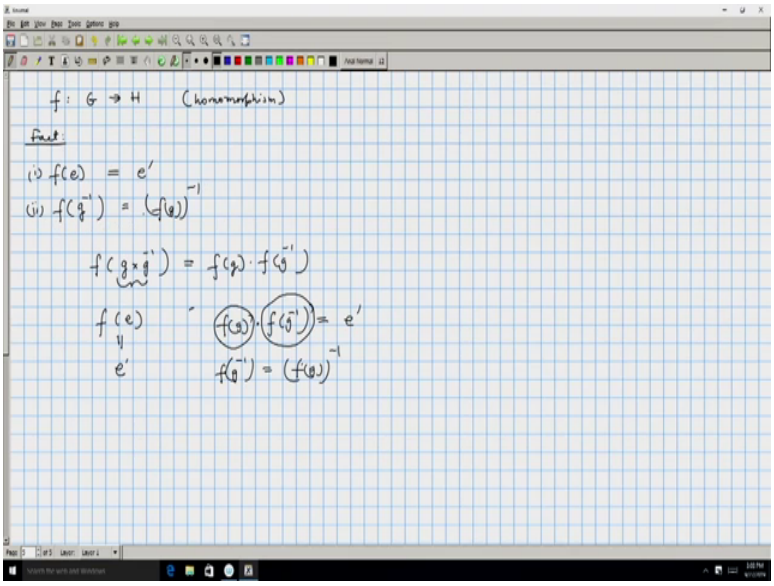
So this is satisfied for all g1 g2 belonging to G then we will say that f is a homomorphism from G to H. okay so suppose G is this and H is some other group and there is a map f and it satisfies this equation 1 then we say that this is a homomorphism. Now while we are studying homomorphism we can restrict our attention to basically the image of f, okay so let us say this is a subset to which f is mapping g2.

We will restrict our attention to just those elements the others does not really matter, okay. So if you call this as image under f, we will just study the effect of the homomorphism by restricting our attention to just the image, the other elements do not really matter or in other words we can say that we were looking at homomorphism which are onto a functions okay. In other words, we will just study those homomorphism where G is mapping to the full set H.

Now there is an easy claim that you can verify, image of a homomorphism will always be a subgroup okay. So even if we have taken the larger collection and if we were just looking at the

image, that will be the subgroup of H. Okay so that is the reason why we can restrict our attention to homomorphism which are onto.

(Refer Slide Time: 15:15)

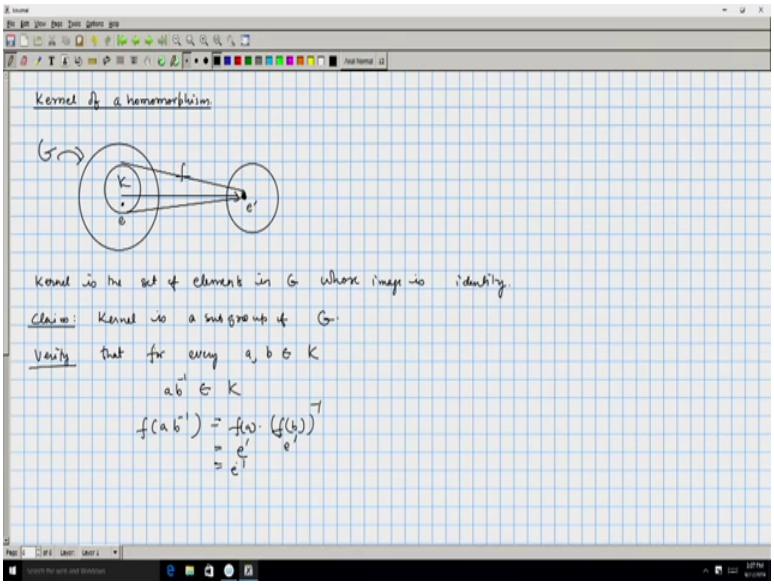


So let us see some properties of homomorphism, let us say if f is a homomorphism of G to H, then f of identity will be equal to identity. It maps the identity in G to the identity in H. And the second thing is f of g inverse, so let say g is any element and if you look at its inverse and look at the image inverse that will be equal to f g inverse, both of these statements are easy to verify, we will just verify the second part, okay.

So let us look at the f of g times g inverse, f by the virtue of being a homomorphism this must be equals to f g times f g inverse and f of g times g inverse, g times g inverse is going to be identity, so this is f of identity okay and f of identity this is equal to identity. Now this is, e is the identity in G and e prime is the identity in H. So what we can conclude is f g times f g inverse, this is equal to identity in H, so this is an element of H and this is another element of H, okay.

So and when they multiply, we get identity that means those elements are inverses of each other. So we can write f g inverse is equal to f g the whole inverse, okay so that basically is fact 2.

(Refer Slide Time: 17:02)

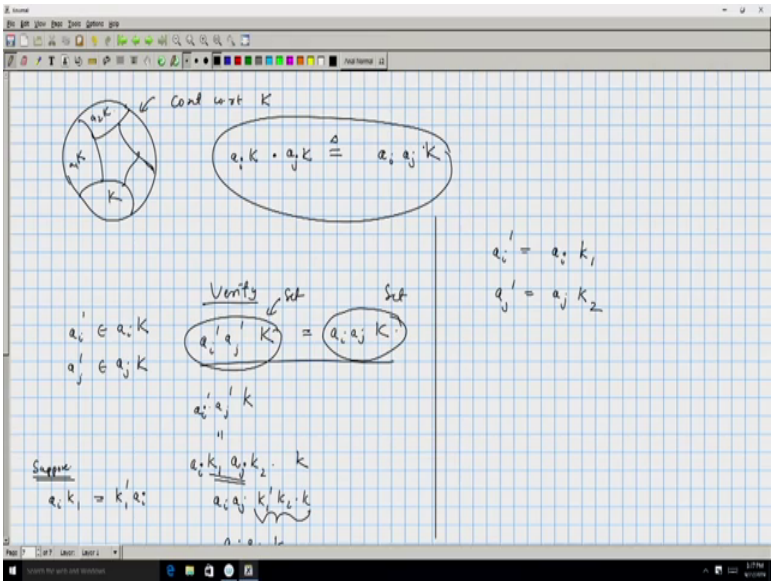


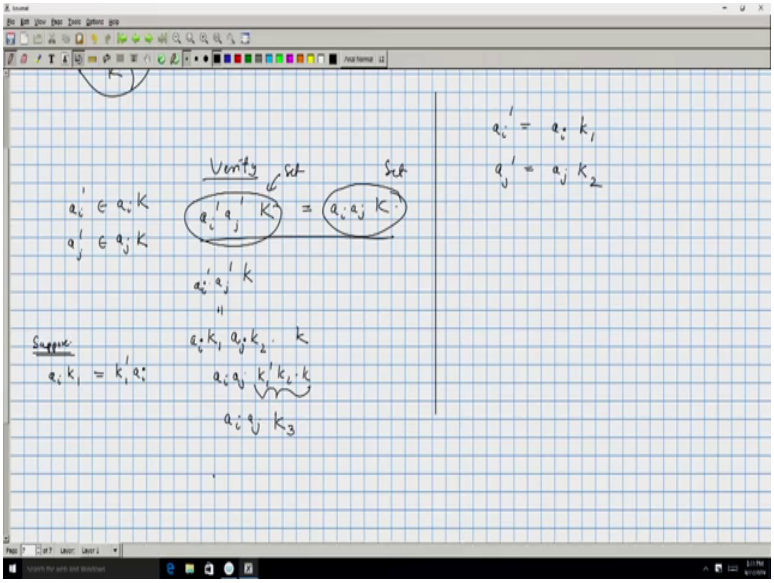
The next concept that we will see, is what is the kernel of a homomorphism. So homomorphism is a map from one group to another which preserves the group structure. And we argued that when we have a homomorphism, the identity will map to the identity. Now we can look at all the elements, there might be multiple elements mapping to the identity, so all of them will be mapped into the identity. That collection is known as the kernel.

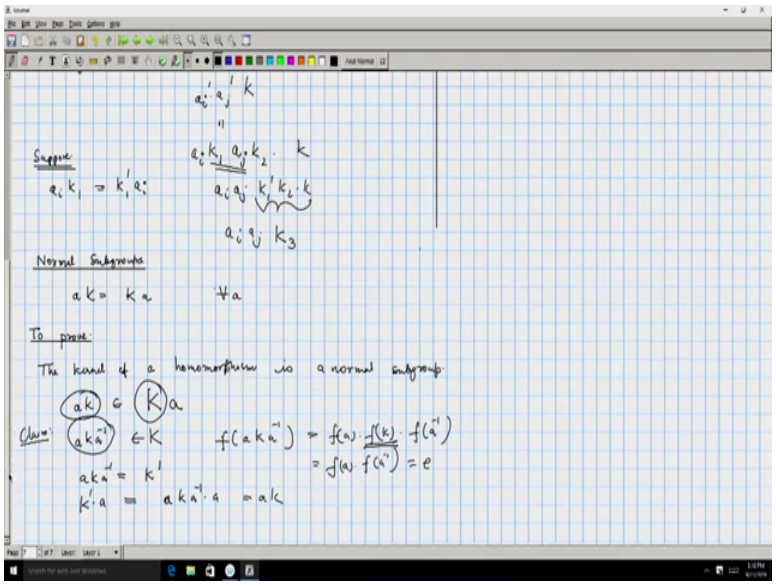
Okay so kernel is the set of elements in G whose image is identity, so the kernel of a homomorphism is the collection of all those elements in G, which maps to the identity. There is a simple fact, kernel is a subgroup of G, we denoted the entire group by G this is the kernel. Okay so kernel will invariably be a subgroup of G. How do we verify that? So in order to verify that a subset of a group is a subgroup, what we need to do is verify that for every a, b belonging to K, a b inverse belongs to K. If you verify this part then we can conclude that the subset is, the subset K is going to be a subgroup.

Now it is easy to check because f of a b inverse, if we can show that this is identity then that means for every a b belonging to K, a b inverse also belongs to K. f of a b inverse is nothing but f of a times f of b inverse which is f b the whole inverse. Now f a is identity, f because a belongs to the kernel and f b also is identity because b belongs to the kernel and inverse of identity is identity, so this entire thing is e bar okay. So kernel is always a subgroup of G.

(Refer Slide Time: 20:09)







Now here we are in a position to state our main result which is a connection between the kernels and the quotient structure. We were asking this question, when can we define a substructure on the cosets? If we look at kernels, kernels we know as a subgroup and we can consider we can construct cosets with respect to a kernel K. So let us say this is a kernel and then you consider its cosets. For this you can (multiply), I mean if you had these cosets a1K, a2K and so on and if you define the operations on these cosets as, so let us say aiK times ajK, so aiK is the coset containing the element ai and ajK is the coset containing the element aj.

And if you define this as a coset ai aj K okay that is the coset containing the element ai aj, now we can verify that this is a valid definition because let us say ai prime is some other element of the same coset and aj prime is some other element of the coset ajK, if we multiply them out, the rule say that they should be equal to ai prime aj prime K but this should also be equal to ai aj K, so this is what we need to verify.

Okay in order to verify this, this is a set and this is another set, when are these sets identical, if you that one is contained inside the other when a is contained inside b and b is contained inside a, then the sets a and b are the same. We will just verify for one direction, the other direction is automatic, the same reasoning would work. So an arbitrary element of the LHS is ai prime aj prime K okay.

Now note that ai prime is equal to ai into K1 and aj prime is equal to aj into K2 okay and therefore ai prime aj prime K can be written as ai K1 aj K2 into K, if we could somehow show

that ai K1 is equal to K1 prim ai, okay so suppose these were true then what we can do is, we can just rearrange the elements and get ai aj times K1 prime K2 prime K and K being a subgroup these things multiplies into some K3, so we will get (a1 aj) and ai aj and K3 okay and that is going to be an element of the set ai aj K okay.

So what we need to show really is that ai K1 is equal to K1 prime ai, okay so this may not be true for arbitrary subsets but the subsets for which this is true have a special name those are called as normal subgroups. So we can assume the theorem to be complete, assuming that a K is equal to Ka, if aK was equal to Ka for all a, then ai K1 is equal to K1 prime ai. So assuming that the kernel is a normal subgroup we done with our proof because this was a normal subgroup then this K1 aj, you can flip that and push the aj to the left side and push the K1 to the right side.

Okay so all that remains is to show that the kernel is a normal subgroup. Okay so how do we show this? So in order to show that some subgroup is a normal subgroup, what we need to show is aK is equal to Ka, so let say, consider an arbitrary element aK and we need to show that aK belongs to Ka. So consider the element a Ka inverse, so a Ka inverse we claim that this belongs to K okay.

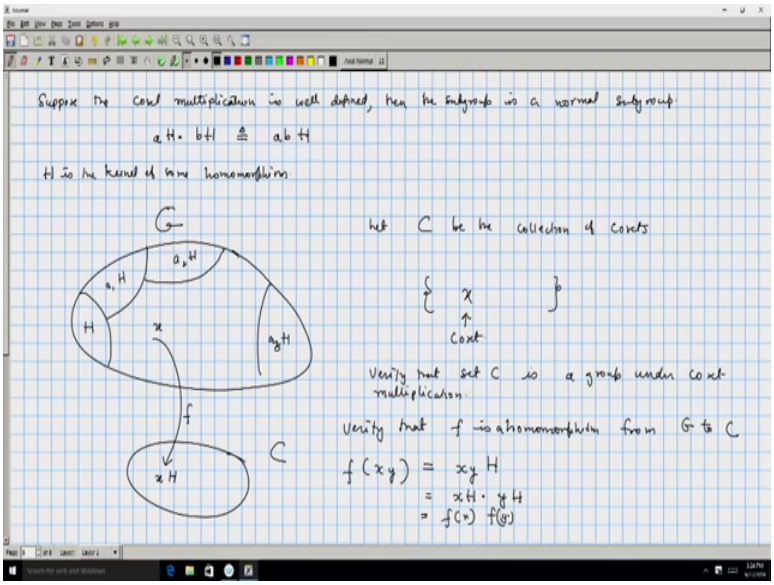
This is because, if you look at the homomorphism f and if you consider f of aK inverse, this is equal to f a times f K times f a inverse. Now f K is identity because K belongs to the kernel, so this is equal to f a times f a inverse and this is equal to identity because f a and f a inverse is, an f a inverse are, inverses of each other. Okay so aK a inverse belongs to K therefore if we take aK a inverse as K prime, okay K prime into a is equal to aK a inverse times a which is equals to aK okay.

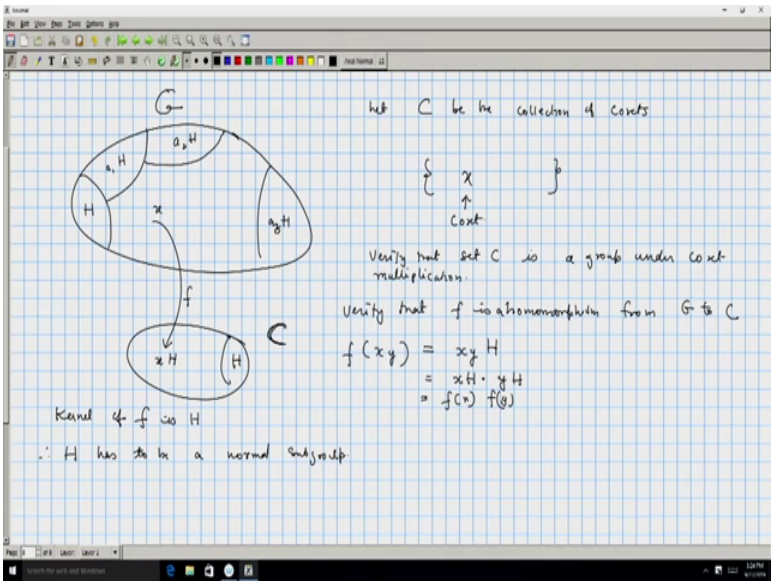
So we have written aK as a product of an element belonging to the kernel and a where the multiplication with a is on the right side okay. So the kernel of a homomorphism is a normal subgroup. So to put things together, what we verified is that, you take any homomorphism, its kernel if you consider the kernel it is going to be a subgroup not just that it is going to be a normal subgroup.

And once you have as normal subgroup, the multiplication of cosets is well defined and therefore that induces a, the homomorphism induces a quotient structure or a group structure with respect to the cosets. And what we will show next is that, this is the only possibility, in the sense if we

can make the cosets into a multiplicative structure, there is a, if this definition of multiplication is to be valid then K must indeed be a normal subgroup.

(Refer Slide Time: 27:12)





Okay so that is the second part, suppose the cosets multiplication is well defined then the subgroup is a normal subgroup. So coset multiplication we define as, if you have aH and bH their product is defined as ab times H. Now this definition is to make sense that means if it is to be well defined then H must indeed be a normal subgroup. The way we would show this, prove this theorem is by showing that H is the kernel of some homomorphism okay.

So we will construct a homomorphism for which H is the kernel, it is easy to construct. So here we have a group and this is a subgroup and the subgroup gives rise to various cosets, cosets let me call it as a1H, a2H and so on. Now let me just consider the collection of these cosets, so let C be the collection of cosets, so C is a set okay and each element of C is a coset and now the, what we have assuming is that the coset multiplication is well defined you can verify that the set C is a group under coset multiplication okay.

Since the operation is well defined we can check whether that operation is an associative operation, whether inverse is present, where identity is present and so on. You can verify all these things and conclude that this collection C under the coset multiplication is a group. So now, let us consider our main group G and consider a function which maps elements of G to this collection C okay.

So an element x is mapped to the coset xH, so clearly every element of C is the image of some particular element in G and we can verify that this function f, function f is a homomorphism from G to C. Why is that so? So f of say xy, this is equal to xy times H by definition f maps any element to the coset containing that particular element and that is xyH. And since our multiplication was well defined, we know that this is nothing but xH times yH and xH is f x and yH is f y.

So we verified that the function f is a homomorphism from G to C and the kernel of that homomorphism is precisely H. Kernel of f is all those elements, which map to the identity element of C, the identity element of C is basically H and therefore, you can verify that every element in the coset H will map to H and therefore, since the kernel of f is H by our earlier theorem H has to be a normal subgroup. So this concludes our study of groups and subgroups and the quotients structure that is induced by a normal subgroup.