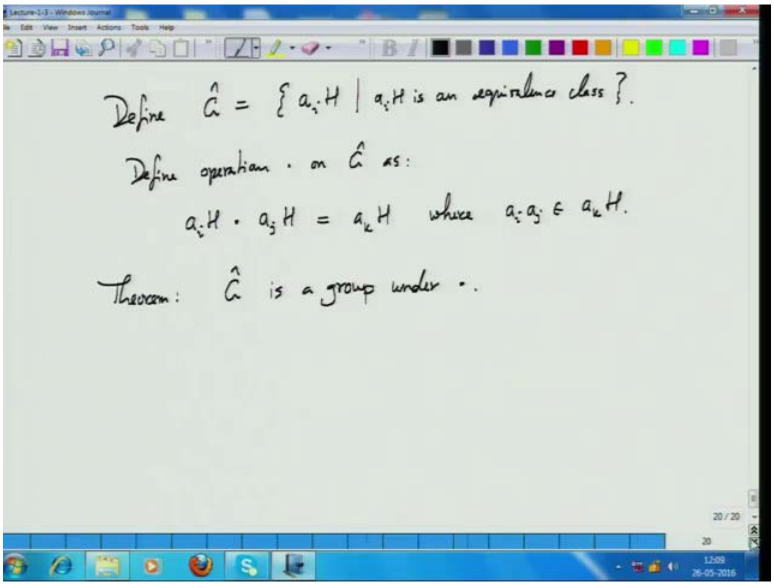
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institution of Technology, Kanpur

Lecture - 04
Groups: Quotienting

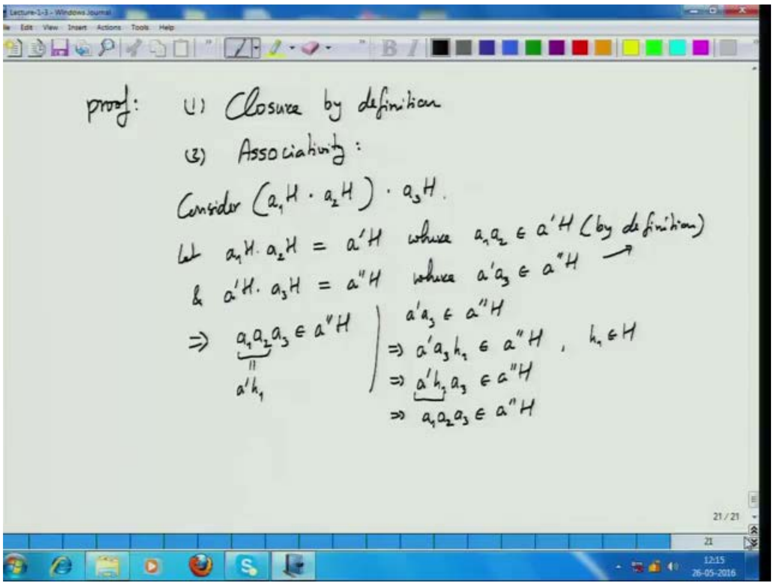
So, last time we left of at this theorem, where the theorem if you see the screen.

(Refer Slide Time: 00:22)



We had defined the set G hat as the set of equivalence classes with respect to the relation induced by these sub group edge on the group G. So, a i H is an representation or a name for 1 equivalence class and we defined an operation dot on this set G hat as the following a i H dot a j H, so this operation between 2 equivalence classes which gives a third equivalence classes a k H and the definition is that a i a j is an element of the equivalence class a k H. That definition is precise and now we want to show that G hat is a group. So, let us prove this.

(Refer Slide Time: 01:20)

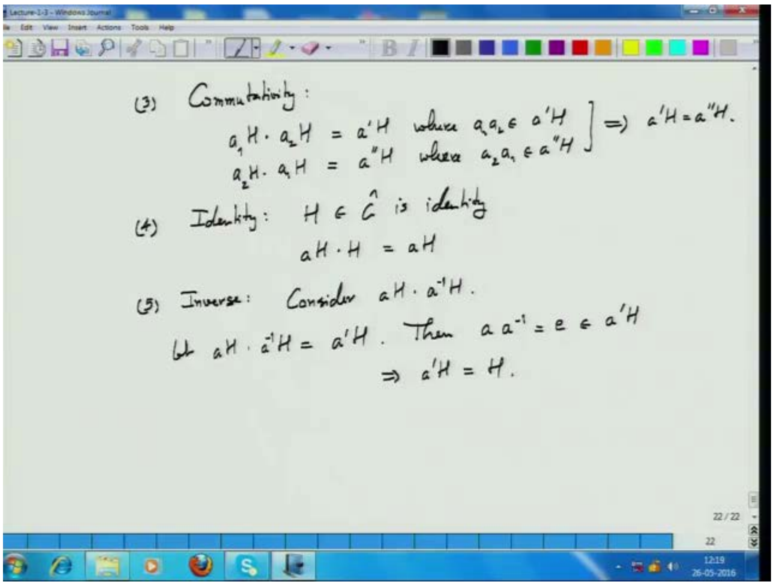


What are the conditions we require for a group? First is closure that is by definition because you see that a i H dot a j H is by definition and element of G hat. So, this certainly closed under the operation dot that is not a surprise at all. Next associativity, so we have a 1 H dot a 2 H and then dot a 3 H; what is this element? You consider this. So, a 1 dot H a 2 H a prime H where by definition a 1 a 2 is in a prime H, and then a prime H dot a 3 H is a double prime H, where a prime a 3 is in a double prime H. This is also by definition, correct.

Now, put these 2 together what is the relationship or what is a double prime H in terms of a 1 a 2 a 3? See a 1 a 2 is a prime H and then a prime H a prime a 3 is an a double prime H. So, we can say why is this, a 1 a 2 is equal to a prime H 1 and a prime H 1 time times a 3 is in a double prime h. So, this implies that a prime H 1 a 3 is a double prime H and clearly you can remove H 1 from here and let us argue this little more carefully. So, we know that a prime a 3 is in a double prime H. This implies a prime a 3 H 1 is in a double prime H, you agree with this because H 1 is in sub group H. This implies a prime H 1 a 3 in a double prime H because it is a commutative and a prime H 1 is a 1 a 2.

So, this is an equivalence class, this product with an equivalence class defined by the element a 1 a 2 a 3, whichever is the equivalence class which a 1 a 2 a 3 belongs to is this product. Now, associativity follows immediately because you see that whether we do the operation on a 1 H a 2 H person then a 3 H or do we a 2 H and then a 3 person then a 1 H that would give us a 2 a 3 a 1 is in a double prime H. Now, again commutativity, a 2 a 3 a 1 or a 1 a 2 a 3 they are all in a double prime H. So, this completes the proof of associativity. Are you convinced? Is there a doubt in this? No, it is pretty straight forward just that I went through the detail because it is important to formally write down this details and verify that for a general problem this thus hold.

(Refer Slide Time: 07:02)

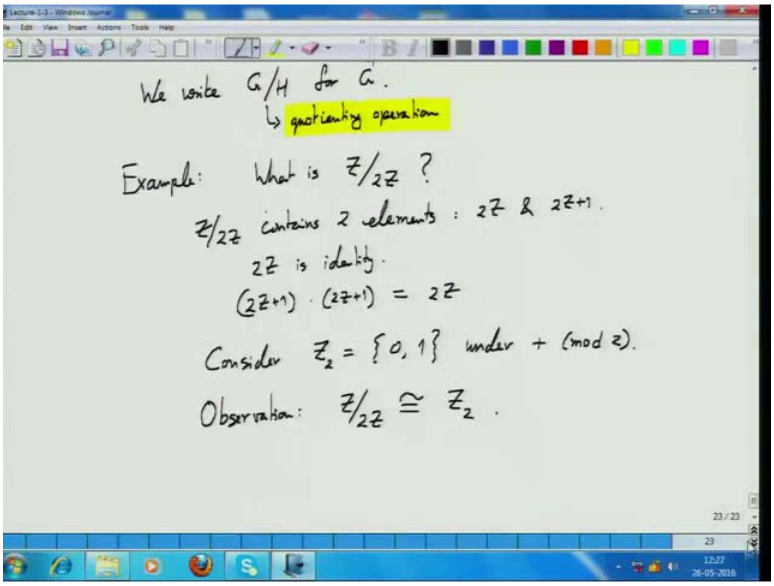


Next, what is the next property? Commutativity. So, we have a 1 H dot a 2 H this follows again almost immediately is a prime H where a 1 a 2 is in a prime H, a 2 H dot a 1 H is a double prime H, where a 2 H a 1 H is in a double prime H and these together a 1 a 2 and a 2 a 1 and again by commutativity are the same element. So, they both belong to the same equivalence class. This 2 equivalence class is always same. Next, identity what is the identity? H is the identity. Why is that? If you have a 1 H dot H, this is H. Similarly, H dot a H again it is commutativity.

Inverse that is the final property. So, what is the inverse of element a H, obvious what at least you can guess it. What should be the element of a H a inverse H less verify that? Consider a H dot a inverse H. Let us say it is a prime H then again by definition a a inverse which is identity is in a prime H and if identity is in a prime H, what does this mean? It means a prime H is H that is only the equalize class which contains the identity element and that is the end of the. So, now, we can see something quite interesting that is happened. We started with a group we identify the sub group of the group and then we introduce the equivalence classes with respect to that subgroup.

From the equivalence classes we made in d set and we define a new operation which is somewhat related to the group operation, but not quite the same because this operation over equivalence classes and it turns out of that new set under the new operation is also, this is a very important process, it is given a name and notation. So, let us define that.

(Refer Slide Time: 11:08)



So, that new group G hat is written as G slash H. This is the division sign and in a certain sense this is what we are doing. We are dividing the group G by the subgroup H because each equivalence classes are now represented by 1 element. So, there is certain amount of division that some kind of division that is happening and that is the sense or that is the reason why we write at this way and that is why we call it quotienting.

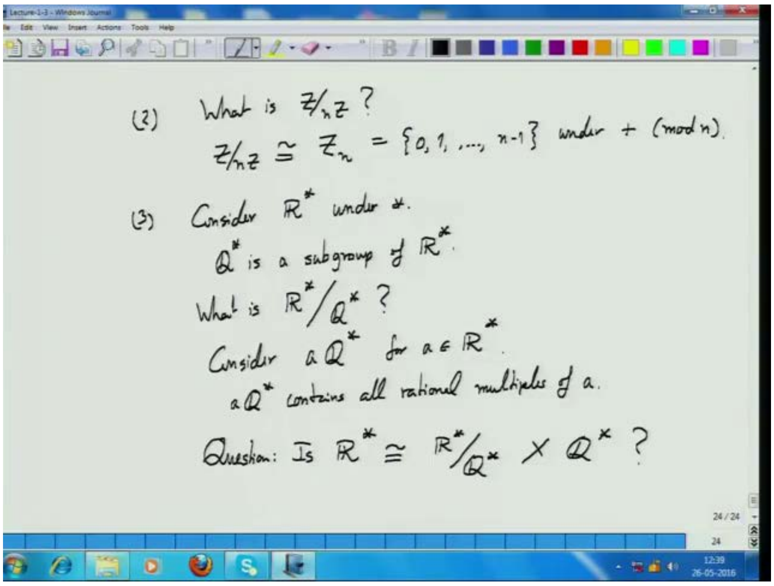
So, this slash is quotienting operation and we of course, always need to quotient a group with subgroup and are result of quotient thing is another group. Now, having seem this let us get back to our motivating example, what we started with was this group of integer and the radiation that we identify a subgroup there are many subgroup that will set of even numbers and that the subgroup, or if you quotient Z by the group of sub group of even integers by this theorem that we proved we must get an another group, what is that group?

Firstly, what are the equivalence classes we will get 1 equivalence class there will 2 Z its self other equivalence classes. So, set of all odd numbers to Z is the all even number that is exactly 1 more equivalence class which is all outcomes. So, this group the new group will have these 2 elements the 0 or the identity would be 2 Z and then they will be the other set of all odd numbers other element. So, what would be the operation on this new group? Let us write the odd number has 2 Z plus 1 as a notation. 2 Z is identify, what is the new operation? How does it look like? So, we only need to work look at the definition of new operation on 2 Z plus 1 itself because this is 2 Z is the identity anything that you operator 2 Z with you get back that element. So, what is 2 Z plus 1 2 Z plus 1 dot 2 Z plus 1 or is this it is 2 Z wait this is 2 Z everything else is defined already.

So, that is it this completely describes this group said by 2 Z. Is this a familiar looking group? Let us define another group Z 2, which is just 2 number 0 and 1 and the operation is addition model two. So, for this operation addition model of 2 is 0 is the identity and 1 plus is 1 is 0 and that is it that completely describes this group. So, do you see similarity between Z to Z by 2 Z? What is the similarity? So, Z to s already have at have notion. Now, this is isomorphic because except for the notation that is am writing 0 by 2 Z and 1 by 2 Z plus 1 nothing else is difference your operation dot is really additional model that excellent.

Let us again let me re elaborate, it we started with group of integers quotiented with a subgroup we got a new group which is familiar to you that is the set of integer model 2 under addition. We can do the same exercise, this is the first example.

(Refer Slide Time: 17:47)



Let us say, we can do a very similar example. Again, let us say take another subgroup of Z. Sorry.

Student: (Refer Time: 17:55).

Yes, in general any subgroup of Z will be of the form n Z that is all multiples of the number n. That is the general form of subgroup of Z it requires the little bit of working out, but you can do that on your own. So, what is Z by n Z? You can work this out in a similar fashion. What will be the equivalence classes for Z by n Z it will be n Z itself will be equivalence class. So, what are the other ones, n Z plus 1 n Z plus 2 n x plus 3 to n Z plus n minus 1. There will be exactly n equivalence classes the group operation would be x essentially model n. So, this is isomorphic to Z n which is the set of numbers between 0 and 1 minus 1 under additional mod n. So, that is the structure of subgroup of the group that you have obtained by quotienting general sub group format from Z.

The one interesting factor about this none of this subgroup as we getting are on other these group we are getting are subgroup of Z, none of these again is a sub group of Z, but by quotienting with subgroup of Z we are getting. So, which basically telling us this quotienting by subgroup is creating new groups and this is the one very good way of creating new groups.

Let us take another example and I would like to seek suggestion from you on which group should we look at to next. You take a group take a sub group quotient it and see what you get. Suggestions, for the next group to be considered; real numbers, real numbers are the addition multiplication. So, non real 0 numbers non 0 real under multiplication, right. Consider R star which the set of all non 0 real numbers under multiplication fine. So, that is finding a sub group? Q is a sub group, Q star. Now, what is R star quotiented with Q star? Very interesting question, what are the equivalence classes?

Student: (Refer Time: 21:46)

That, it is isomorphic class to R star, it would not be R star, but one can ask is it isomorphic to R star. Firstly, we can worry over it later; let us identify the equivalence classes. What are the equivalence classes under this quotienting? So, take any equivalence classes here, of course one will be Q star itself, but take any other equivalence class. So, let us consider some a Q star for some real numbers or non-zero real number. So, what are the elements in a Q star? By definition element of a Q star are going to be of the form a times irrational number. So, elements of a Q star therefore, are all rational multiple of a.

Now, I quotient this out so that means, each equivalence class represents a real number and all its rational number and now we can talk about operation between different equivalence classes. What would that give us? Take each equivalence class is represented by a real number a, we can say a represents a Q class and if you multiplied to a 1 a 2 to real numbers you will get a 1 times a 2. Is a 1 times a 2 a different equivalence class or can it be the same equivalence or 1 of the same equivalence classes? It will be a different equivalence class because a 1 and a 2 you cannot be rational multiplication other. Otherwise they would be in the same equivalence class.

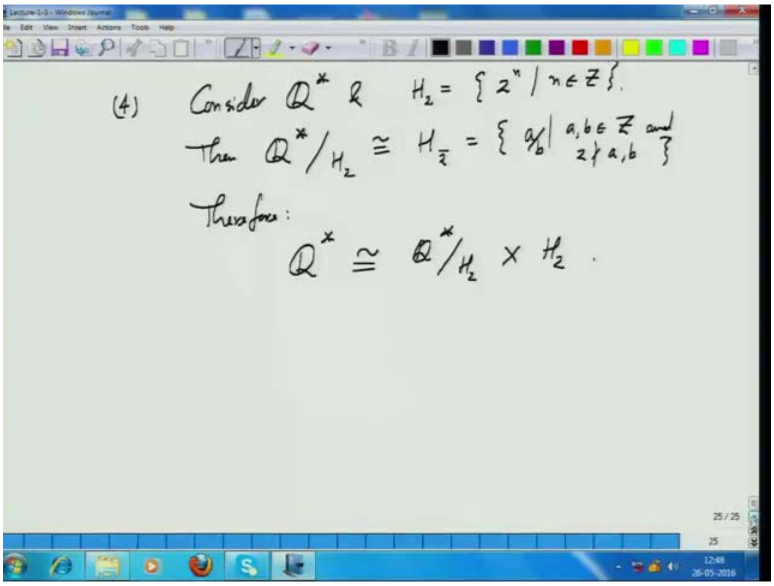
So, even in fact, a 1 a 2 are rational multiple of each other that is they are the same equivalence from the same equivalence class their product is a 1 a 2 times always all is rational multiples. So, a 1 a 2 not be rational multiple of a 1 or a 2.

Student: (Refer Time: 24: 55).

Unless you are going with rational, which means that one of the reasons is identity plus which is then; obviously, it will be the property. So, essentially in this group operation will get we get subset of real numbers such that no real number is a rational multiple of any other real number. So, you collect all such real numbers and then the just define the multiplication operation between of them real numbers and that is the subgroup that we will get. So, this is a different subgroup than R star is different group than R star. It is, we can view it as a sub is a kind of subgroup R star by its a different 1 because for a example integer do not existence what will happened to all integers they are in Q star. So, they all are essentially collapsed into 1 single identity element that is 1. So, all integers collapse to 1, in fact all rational number collapse to 1.

It is a strange kind of a subgroup that you get, but it is a something which is not. So, obvious to see a less we has a quotienting operation. Here it is a question, Is R star isomorphic to this quotient group product with Q star? This is not always true.

(Refer Slide Time: 27:17)



For example, integers, for example, we know that integers are not isomorphic to 2 Z cross Z by 2 Z. Why do we know this because Z by 2 Z this is subgroup of z, but Z by 2 Z is not a subgroup of Z and by definition, the product exist when only if you can split a group into subgroup and product of 2 subgroups. So, there is no subgroup of Z that is isomorphic to Z by 2 z. So, it Z is not isomorphic to Z 3 at times it is not in this case, but for other certain other groups it is let through for highlight that.

Let us takes the next example, which is somewhat less satiric than last one. Just consider Q star as the starting group Q star and its subgroup of Q star which is let us say all parts of 2 we had something to do with this particular subgroup earlier let we write this as H 2 as 2 to the n, n and Z all positive negative parts 2 this is subgroup of Q star by you have seen this quotient Q star with this what is this again it is this again something you have seen let me pull go back I use the name H 1 there H 2 was for the rest. So, am choosing a different name which is thing slightly better in name because you have 2 represents of all powers of 2 we are taking of and what is the quotienting of Q star by H 2.

Just think by definition it is saying it contains a rational the each equivalence class contains all rational numbers that differ by a power of 2 by multiple of a power to switch. So, each equivalence class can therefore, be represented by a rational number which is not divisible by 2. When I say divisible the essentially prime factorization has no power of doing it positive or negative and then again that is also subgroup. We saw that last time there is and then I am going to write again using slightly better notation H 2 bar 2 bar means get rid of 2.

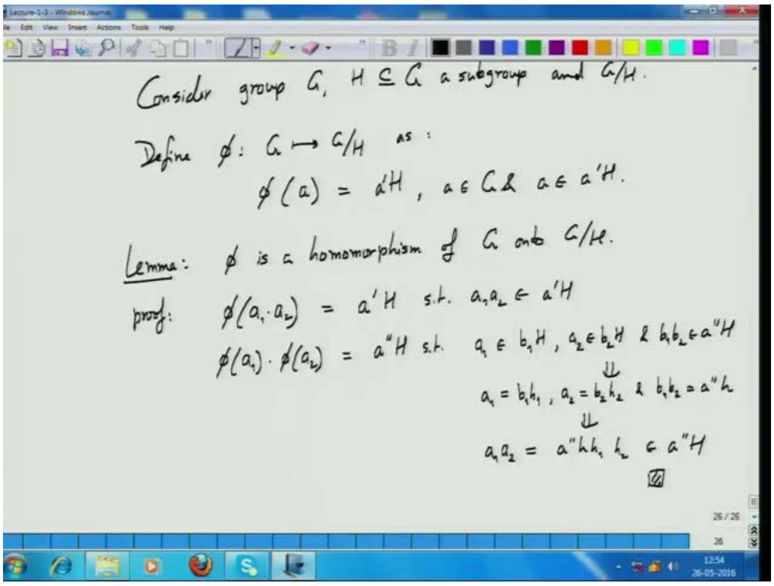
This is that of all rational number such that a is in Q star and or say a by b sorry a by b is in Q star or it mean better still write it as a b is in Z and 2 does not divide a or b and you see that this subgroup that you will get the equivalence class. So, this is should write it has equal to, but it is isomorphic. So, equal I cannot really write Q slash Q slash slight as to is a collection of equivalence classes that not really collection of all numbers, but just like we can establish isomorphism in the integer case, we can establish an isomorphism between these 2 and we also have we can write Q star as isomorphic to Q star slash H 2 times H 2 this our earlier that Q star can be split as a product of H 2 n H 2 bar and H 2 bar is an isomorphic to Q star slash H 2.

What we have seen or learnt here is that there are distinctions between groups of this kind. Earlier, we have saw that the distinction between groups either some can be split as a product of subgroups and some cannot be split as product of a subgroups they are the same distinction is being rephrased in another terminology, which is using quotienting that is we split it group as its isomorphic to being this quotient times that subgroup that we are quotienting, sometimes you can do this like here, sometimes you cannot do that and coming back to this question I will leave this as an assignment problem, please work this out.

You should be able to prove it in both ways that is whichever way is correct if it is isomorphic to these you should able to prove with. If it is not isomorphic that should also you should able to prove which means that is quotienting sometimes gives us new groups sometime it does not like in case of Q star quotienting with H 2, we do not get any new group we already present as a subgroup of Q star, but there are cases in where for integer where we. So, quotienting is therefore, very important operation we will see its importance in subsequent lectures as well and we will establish this is one of the really important fundamental operation in algebra.

Now, this is this importance is further in has by his connection with homomorphism. So, actually if you recall I started with homomorphism then kind of switch to this and the reason I switch to this was because I wanted to find out the connection that what to homomorphism between 2 groups as to say about quotienting. What is the quotienting had to do with a homomorphism? So, and the answer is very interesting.

(Refer Slide Time: 35:00)

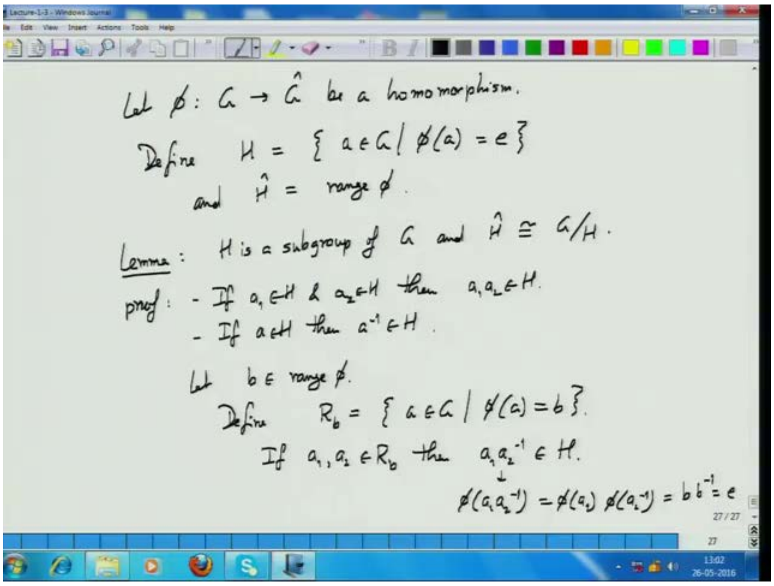


Let us consider group G, subgroup of G and quotient. So, here are 3 groups that we consider. Define a bar from G to G slash H as phi of a is a H that is it or actually this is a H may not as a name exist. So, I should make it little more presides phi over H is a prime H where, a is in G and a is in a prime H. So, this map is actually a homomorphism of G on to G slash H. It is clear that phi is an on to map, that is for every element a H in G slash H there is an element in G that phi maps it to. So, if your element a H then sorry element an of G is certainly mapped to this. Why is this homomorphism? Well, let us verify this.

What is phi of a 1 times a 2 that is some a prime H such that a 1 a 2 is contained a prime H right and what is phi of a 1 dot phi of a 2? This is desiccate our a prime H such that phi of sorry a 1 is contained, let us say b 1 H a 2 is contained in b 2 H and b 1 b 2 is contained a double prime H. All by definition, a 1 is contained in b 1 H a 2 is contained in b 2 H and b 1 b 2 contained a double prime h. So, what about a 1 a 2? This implies that a 1 is b 1 H 1 a 2 is b 2 H 2 and b 1 b 2 is a double prime say H. This implies to this analysis a 1 a 2 is a double prime H, H 1 H 2 b 1 is a 1 H 1 inverse b 2 H 2 inverse. So, just substitute it here and we get this.

Now, clearly this is a double prime h. So, a 1 a 2 is contained a double prime h. So, if phi a 1 a 2 is therefore, equal to phi of a 1 dot phi of a 2 that is the proof that phi is a homomorphism. It is not a surprise when the way we phi was defined it is was essentially this using the fact already observed that of G slash H is an group under that new operation we are defined and it is really a is a restatement of that. So, this says that we have a group and the quotient group where is in a homomorphism which takes a group on to really, what it this come to action look at the each equivalence class of G under H is contracted to 1 single element of G slash H and that is the map. What is more interesting is the converse.

(Refer Slide Time: 40:32)



Consider any homomorphism from G to G hat. Now, define 2 sets H to be all elements in G such that phi of a is identity and H hat to be range of phi hat, and we have the sum of that H is a subgroup of G and H hat which is a range of phi is isomorphic to the quotient group of G slash H and this tells us there is essentially homomorphism in new sets a quotienting of the group on which it is operating. Quotient a group with a subgroup and the output on the range produces the quotienting.

Proof, a very simple proof it is this is little bit of manipulation. Why is H is the subgroup of G is very easy to see there is closure property there is if H a 1 is in H and a 2 is an H then a 1 a 2 is an H because phi of a 1 is a identity, phi a 2 is identity and then phi of a 1 a 2 by the fact that phi is a homomorphism equals phi of a 1 a 2 is identity. Then associativity it just follow some associativity of G itself. Commutativity of G follows commutativity of G itself. Identity that is identity of G is also in a, because phi being homomorphism will map an identity to an identity. Have you seen this why would homomorphism always map an identity to an identity?

Student: (Refer Time: 43:38)

Yeah. So, phi simple, phi a dot e is phi a dot phi e and which means phi a is phi a dot phi e. So, phi a can be cancelled on both side by multiplying with phi a inverse and therefore, you get phi e is identity. So, identity is same and inverse if a is in H then a inverse is also in H, why a is in H phi of a is an identity that means, phi inverse of phi a inverse identity and therefore, phi of a inverse is also identity, that is it. So, H is the subgroup H n by definition of H phi maps H to identity element is précised the subgroup that is map to the identity element.

Now, let us look at the range of phi. Let us say, let b is in range of phi. Define the set, let us say R b to be all elements of a is in G, so that phi of a is b. So, collect all elements in a in G that are map to this element b of G hat. I want to show that this R b is 1 of the equivalence classes of G when quotiented with H and for that to show I need show that if a 1 a 2 is in R b then a 1 a 2 inverse is in H. You see this trivially so, what is phi of a 1 a 2 inverse. This is phi of a 1 phi of a 2 inverse, this is phi of a 1 is be what is phi of a 2 inverse phi of a 2 is be phi of a 2 inverse b, b inverse and that is identity.

So, a 1 a 2 inverse is an H and that is it that shows that all elements of G that are map to the element b are precisely the equivalence class and equivalence class of G induced by H, and therefore, the range of phi which is H hat is an image of the that G slash H. Each equivalence class is represented by 1 element of H hat and the operation on the again the same because is a homomorphism, the operation of equivalence class is on G side is mimicked by the operation on images on H hat on the G hat side. This I am just stating, I am not writing down this will be good exercise for you to go back and write it out and verify convince yourself.

Another thing which I have skipped for homomorphism, it is again a simple fact which I would ask you to verify yourself is if phi is a homomorphism and phi of a is b then phi of a inverse is be inverse, verify this? So, that is the relationship between quotienting and homomorphism and again it show what we proved shows that these are again different ways of viewing the same phenomena that quotienting can be related to or connected with in a homomorphism and vice versa. So, when we say we want to study quotienting of group, we might as well see you want to study homomorphism between twos. So, this that is makes homomorphism also of equal importance and again we will see later on many more application of homomorphism.

We will break for today and we will meet tomorrow.