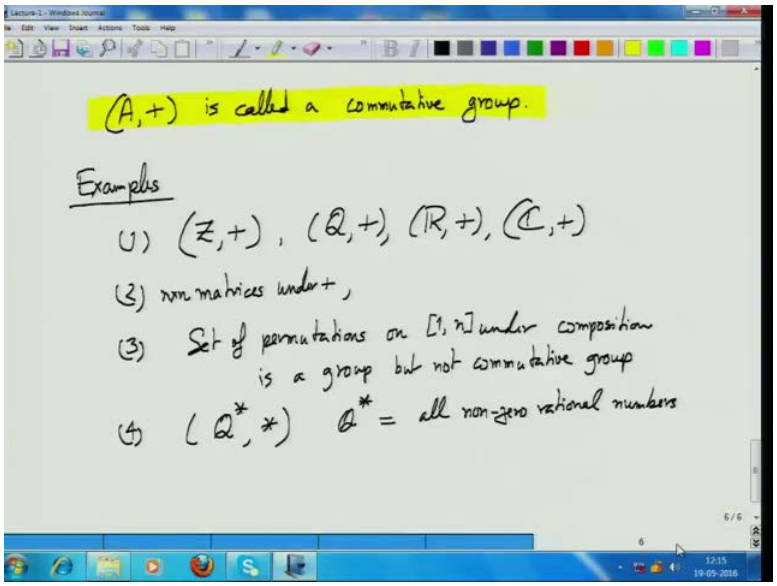
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

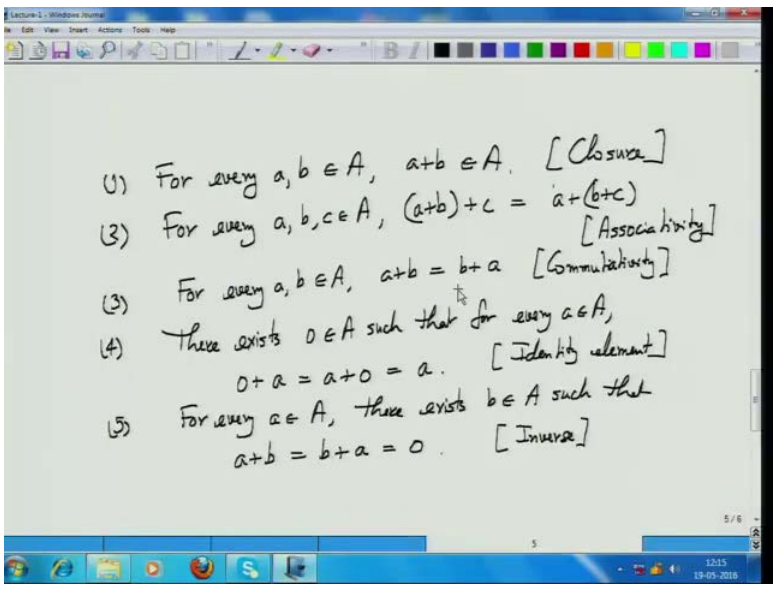
Lecture – 02
Groups: Subgroups and homomorphism

(Refer Slide Time: 00:13)



We looked at the definition of a commutative group and also a group, which I have not written down here.

(Refer Slide Time: 00:30)



But I assume that is every clear that except for the property number three here, which is commutativity, all other property that are satisfied, which is the case in for example, three here; all other examples that we looked at yesterday were commutative groups. Now, in this course, we will primarily focus on commutative groups, there will be occasions when I talk about non commutative groups are general groups. But mostly, we will stick to commutative groups and that is why I had given the definition of commutative group first. Now of the two examples given yesterday, the first one, which is numbers under addition, is a natural obvious example of a commutative group that is how we actually derive the properties of the group as well.

But if you look at the fourth one, that is already a bit of a surprise, because it is a group of nonzero numbers under multiplication, it is a commutative group. Because it satisfies all the properties as we had listed down. We are but the nature of these two operations addition and multiplication seems very different. What we have learned from this abstraction is that while on the face of it these two operations look very different at the certain abstraction level they are the same and that is a first important learning we have. Already we had seen the benefits of abstraction, now we can actually look at both the operation with the same perspective.

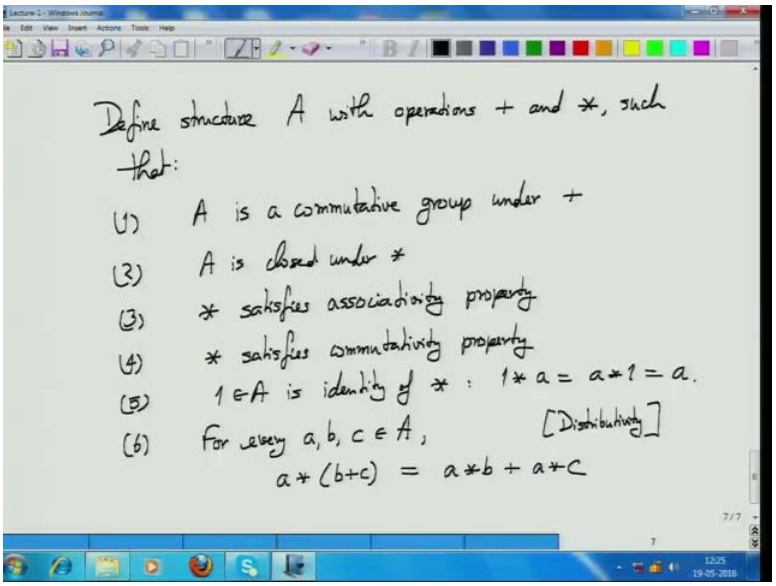
So, now that we have defined what a group is there are two directions in which we can proceed. First one is to continue with our abstraction process, which we started with numbers. Right now, we are only at a half way stage, because we have just seen abstracted out the addition operation property or multiplication operation property as well may be. But we have not talked about the entire arithmetic, remember these numbers admit both addition and multiplication operation, and we do not yet have a definition of a structure in an abstract way, which admits two operations addition and multiplication. In the other direction would be the way to just start focusing on groups and see what are the properties of groups. So, what I am going to do is very quickly I will do the full arithmetic abstraction. Then we will shift our attention to groups, and then later on once we are done with groups we will move on to the full arithmetic abstraction.

Let me first give some at least an abstract it out and give a definition. So, for a full arithmetic to happen over a set of numbers, we have to define two operations - addition,

multiplication and then of course, addition comes in conjunction within subtraction, and similarly multiplication comes in conjunction with division.

Now with division, we have already observed in certain set of numbers division is not possible. For example, integers division is not possible. So, with division, there is always this bit of let us say carefulness that is needed to distinguish this cases where division is possible and where division is not possible. So, let us first define a set of or a structure, which may or may not have division, which is more general types of numbers which you know span everything. So, what are the other properties that we need, just like we identified for groups we had these five properties for addition, surely when we are talking of two operations addition should still retain those properties.

(Refer Slide Time: 05:09)



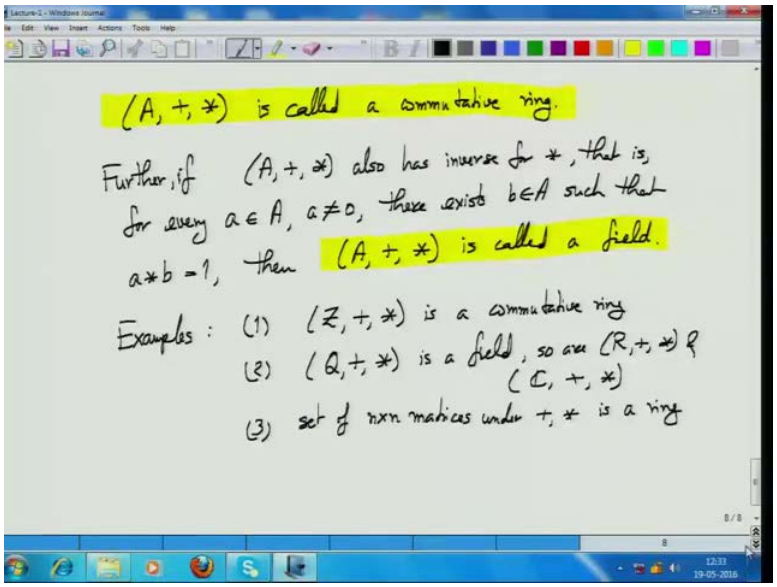
Now let us define a structure. So, I will have two operations addition and multiplication. Such that first A is a commutative group under addition that is again borrowing the property from numbers addition is a commutative. Now, let us bring in multiplication we should not say that A is commutative group under multiplication although there are certain types of number where it is true, but we do not want to say that yet. So, what are the the let us look at integers and what are the properties that integers satisfy multiplication satisfy for integers. If we just go backward to the group properties, we will see that A is closed under multiplication.

Then the associativity holds for multiplication, multiplication satisfies commutativity property a times b is times a. Then there is the identity also present again I am simply picking a property from the definition of groups. The identity is 1 before multiplication the only 1 that I have left out is the inverse, because in words again may or may not exist that is all keep saying that again and again. So, let us give out inverse, because we want to capture numbers in general. Is there anything else?

Student: (Refer Time: 08:19)

Yes, because there is the multiplication and addition interacts in a certain way and that we have not yet captured. And that is captured by a very simple property called distributivity, which is that; for any three elements a, b, c (Refer Time: 08:59), a times b plus c is same as a times b plus a times c it is again very obvious property that multiplication and addition satisfy and that we want to carry your or abstract out. This is called distributivity property that is it. That is the structure with of two operations, which may mix the arithmetic operations over numbers.

(Refer Slide Time: 09:50)



So, structures like this which is now addition and multiplication. So, we have a name for this it is called a commutative ring. Again the commutative prefix is because multiplication satisfies commutativity property by definition in a ring addition is always commutative, it is only multiplication that may or may not be commutative and if it is commutative with the ring is called a commutative ring if it is not commutative it is just

called a ring. And just like with groups we will almost always be concerned with commutative rings in this course, so that is why we are defining it first. Any questions on this?

Student: If you are (Refer Time: 11:00) then it is valid.

Well, you are right in there in certain mode general definitions of a ring the multiplicative identity may not exist, but we will not define it in that general sense. So, we will always assume that multiplicative identity that is one exists. So, this abstraction tells us that set of integers under addition and multiplicative operations are a commutative ring.

So, either set of rational numbers, real numbers, complex numbers etcetera, they all are commutative rings some of them even admit division. So, that is a next step or next definition that I want to define that is third definition. That in case this structure, which is a commutative ring also has inverse for every nonzero element inverse that is the under multiplication, which is another way of saying is that for every a, and this collection, which is nonzero there exists b, so either a times b is 1. This defines division because 1 by a is b.

In that case, the structure is called a field, examples of this whole set of integers under addition; multiplication is a ring is a commutative ring. If you look at rational numbers under addition multiplication, that is a field. So, are real numbers under addition multiplication and complex numbers under addition multiplication? We are going back to yesterdays example set of n cross n matrices under matrix addition and called matrix multiplication.

What structure is that? We saw that under addition it is a commutative group? How about multiplication does it, let us see closure property at is it there associativity a there we have seen that a times b times c there be whichever where you multiply, you get the same result commutativity not necessarily true, identity yes the identity matrix with the identity element.

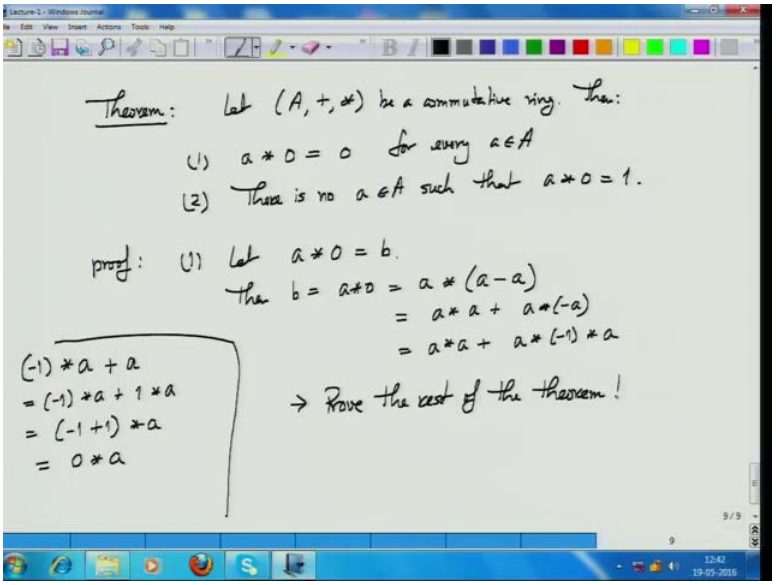
Then finally, for the field the inverse not necessarily true, so matrix may or may not be invertible. So, this is a ring not a commutative ring it is a ring. By the way why have I not included inverse of 0, I say that for every nonzero element a where I defining a field

every nonzero element it has an inverse. What about 0 well for numbers certainly 0 does not have an inverse, there is 1 by 0 is infinity, which is not a number. But that does not rule out a general when we have abstracted it out. So, could it be possible that there exists a set of different set of numbers with arithmetic on them such that there is a multiplicative inverse of 0.

Student: (Refer Time: 16:43) if that is true then.

0 into a is 0, that is another interesting observation is it true it is true for numbers, but is it true for a let us say a field or a commutative ring.

(Refer Slide Time: 17:04)



So, let us prove a theorem our first theorem. We can prove both the problem, let us try to prove the first 1 a into 0 is 0 for every a how do you prove, that this is a good exercise, because while we can try to take the intuition from numbers we cannot be working on numbers. Here we are just working with symbols with a certain properties. So, we have to keep that in mind. So, how do we prove a times 0 is 0, it is very simple let us say a times 0 is b then b is a times 0, which is a times 0 is by definition of 0.

Then in negation (Refer Time: 19:09) take any element let us say c in or why c take a itself then 0 is a minus a. So, I can write 0 as a minus a. Now use distributivity property of multiplication over addition see although I have written it here a minus a it is really a

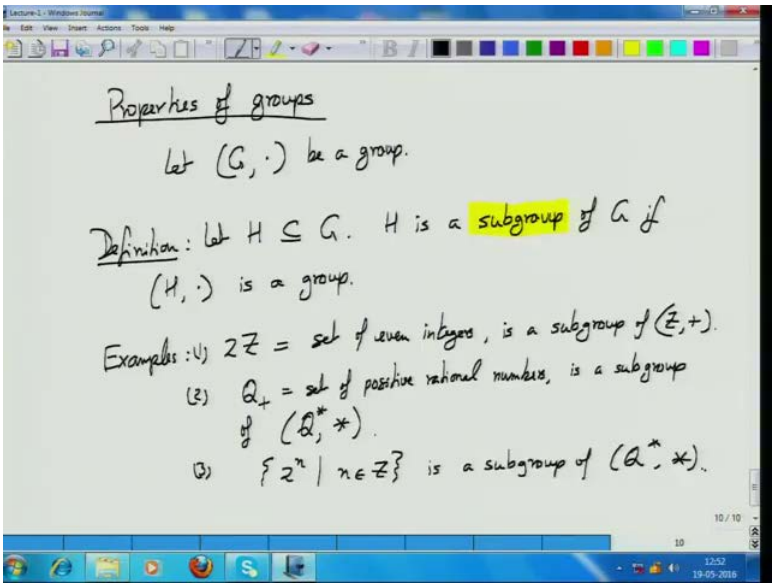
plus minus of a. So, I can distribute this multiplication. So, that is a times a plus a times minus a.

Now, what is a times minus a is it minus of a times a or numbers of course, yes because these are not numbers of the kind that we are familiar with. So, we will have to prove this. Can I write it this way is minus a minus 1 times a should be, but is it. Are you see it is obvious is it obvious nothing is obvious we have to prove every is like learning arithmetic in class 1 due to redo that learning, because although these structures are similar to number they are not really numbers of the kind we know of. So, let us therefore, I do I have to open another (Refer Time: 21:06) that is look at minus 1 times a and I want to prove that it is minus a. So, add a to it, this is minus 1 times a plus 1 times a that is because a 1 is the identity of multiplication.

Now by distributivity property this is minus a minus 1 plus 1 times a and there is 0 times a and what is 0 times a that is what we are trying to prove. So, we have cycled back to that original question. So, we are still stuck we can prove one of them we will prove the other one, but this way we cannot prove any of them, because one property is dependent on the other property. So, we need to come up with an alternative way of proving alright. So, let me tell you what this is an excellent assignment problem. So, I will instead of proving it here which will which when I give the proof and you just. So, write it down it will be very useful if you prove it yourself just play around with these symbols you have all the properties at your disposal and try to prove this. So, prove the rest of the theorem.

But we will take the statement of the theorem as given to us as proven that is and which means that a times 0 is 0. So, which means that when once you prove one, two is very straight forward second property that a times 0 cannot be 1. So, 0 has no multiplicative inverse. So, the collection which is why in the definition you know I have to explicitly write that multiplicative inverse exists only for nonzero elements, so that is commutative ring and field. We will now not talk about rings and fields until some more time we will pick this thread up once we are finished with groups, because in order to understand rings and a fields we first have to understand groups, because under addition there is a group called sitting in both of that. So, let us try to understand groups first and their properties.

(Refer Slide Time: 24:21)



Now, let us for the study of groups let us try to or let us adopt certain notation. So, the structure that we will represent as groups typically we use the capital G to denote the set of elements or objects and the group operation, which earlier even I gave the definition I use plus. Now, I am going to use dot as the representative group operation, this has certain logic to this. Because generally the addition operation in whatever context we use it is commutative, but multiplication operation depending on context may be commutative may not be commutative we see in examples so that that composition which is also denoted as multiplication or matrix multiplication that is not commutative.

So, when we talk of a general group which could be commutative or not commutative it is better to use a multiplication symbol as it is operation and that is why we have we write groups multiplicatively more often than we write them additively. So, let G dot be a general group, now when we want to study a structure what exactly are it is property what exactly should be we looking for one very important aspect is to the structure of the group how really does it look like.

Once if we have understood the structure of the group then we can derive the properties of the group lot more easily. But what does it mean to say what the structure of a group well structure is a like in a sense it certain specific properties like structure of integers you can visualize them as lying on a number line equally spaced and there is a each next

point can be achieved by adding 1 to the previous point. So, that is basically they have to denote the structure of that particular group.

So, in general if G is a group we would like to understand what is the structure and one very important aspect of that is to see if within the group G, if there are more groups and let us that is question is important enough to have it is own definition. So, let us define that take any subset H of G it is a subset of elements of G and we call this subset is subgroup of G. If H under the same dot operation is a group, examples it is always good to have a certain connection of these abstract entities with actual ones. So, for groups it is good to keep two example groups in mind one is numbers under addition, the other is numbers under multiplication and they both are groups, but both have it is very different structure as we will see as we will see later on. So, examples in integers over addition are there is subgroup in that.

Student: Even integer.

Even integer yes, excellent yes 2 Z, which is set of is a subgroup, how about numbers under let us say rational numbers under multiplication you see as a group pair.

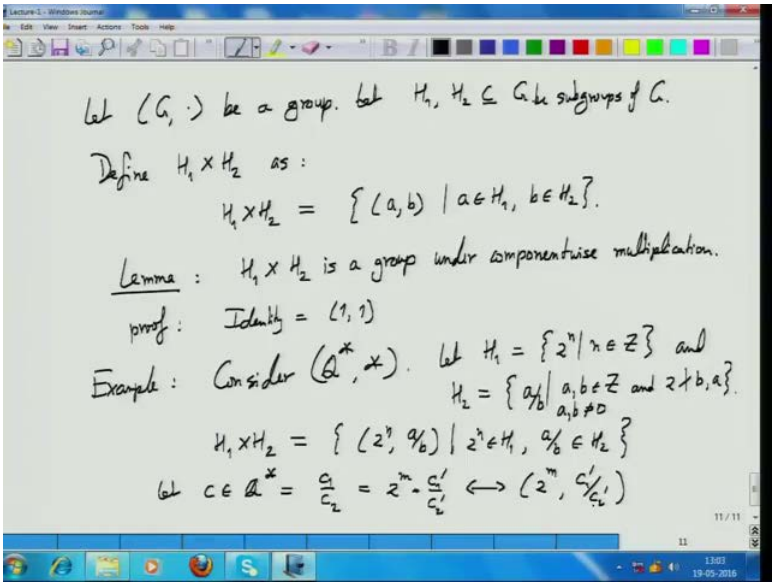
Student: (Refer Time: 30:25).

Positive, positive rational that is subgroup under multiplication that is right; so is a subgroup of Q stars, Q star is defined as a set of nonzero rational numbers. So, we do have subgroups and in fact, these are not the only subgroups that you can find these groups. So, you can have 3 Z is also a subgroup 4 Z is also a subgroup called relation. For group rational numbers under multiplication, you can again create lot of other subgroups. Again let us see the examples being called let us say this set two to the n n is an integer is a is a subgroup of rational numbers under multiplication, do you see this it is straight forward, where you can multiply any of these two elements it is closure and all other property they are also satisfied. So, subgroups of a group tell us a lot about the structure of that group.

In fact, there is one very important way of writing a group in terms of it is subgroups, because just imagine the following here a group you identify is a collection of subgroups of that group. Each subgroup is in a sense smaller than the group itself and you keep identifying further subgroups of that. Until you when you it is possible that this process

can continue, forever it is also possible that this process stops after sometime. In either case you have a very a nice hierarchy of subgroups of that a group and that structure of that hierarchy will tell us the structure of the group itself. So, one very nice way that this hierarchy is that times defined is when I can write a group as a direct product of two subgroups, let me define that.

(Refer Slide Time: 33:36)



So, let G be a group and H 1 H 2 be subgroups of G. Now I am going to define what is called the direct product of H 1 and H 2, which you written in the H 1 cross H 2. It is simply a pair of elements a, b, where a belong to H 1 and b belongs to H 2. In fact, instead of calling it observation let me this is really a lemma H 1 cross H 2 is a group under component wise multiplication, you understand what component wise multiplication is.

The elements of H 1 H 2 are pairs, so with two given to such pairs you multiply them component wise and there is a natural way of doing it because first component belong to H 1 second component belongs to H 2 and there is a multiplication operation defined both on H 1 and H 2. The nice thing or interesting thing is that this is a group, why you can quickly run through all the properties closure trivially there, associativity trivially there because component wise component wise it is basically we are borrowing properties of H 1 and H 2 closure associativity well and if H 1 H 2 are commutative then. So, is this commutative or if not then wrong. Then identity, what is identity.

Student: (Refer Time: 36:48).

Identity is.

Student: Identity of a pair (Refer Time: 36:55).

Yeah the pair 1 comma 1 good the identity of H 1 identity of H 2, which both happen to be the same, because they are both subgroups of G. In words again the borrowed from H 1, H 2 is everything is just borrowed from H 1, H 2. It is clearly, therefore (Refer Time: 37:12). This itself does not tell us something very interesting just we have seen a way of creating a new group from given two groups. You then use correct product, what is interesting is the following, that is if G can be written as H 1 cross H 2 by that, what I mean is every element of G can be uniquely identified with an element of H 1 cross H 2; such that, when we do the operation on elements of G that is exactly the same operation that we do on H 1 cross H 2.

So, we already define a group operation on H 1 cross H 2 that operation and the operation of elements on G they are identical. You see what I am trying to say. Now then let us do an example let us say consider Q star under multiplication and we define H 1 to be 2 to the n, n in Z and H 2 to be all rational numbers in Q star by b, which is a rational number a, b in Z and 2 does not divide a or b. Of course, I have to say a, b not zero also. So, H 2 is all those nonzero rational numbers. So, in that 2 does not occur in the numerator or denominator as a multiplier, so that is both a and b are odd numbers that is a simpler way of what we are saying is this a subgroup of Q star under multiplication yes or no; if yes, then why?

Student: (Refer Time: 40:06)

b by a.

Student: Yeah

Of the same form odd by odd?

Student: Yes, then identity is 1 by 1.

1 by 1 again same, correct.

Student: And then you are putting an (Refer Time: 40:17).

The only one thing is I think the key thing is the closure a by b times a prime by b prime it is set a, a prime is odd. So, their product is odd b, b prime is product is odd and therefore, everything you see takes care of itself. So, this is also a subgroup what is H 1 cross H 2 is a pair collection 2 to the n times a by b right. Now, comes the key point look at any element of Q star. I can write it as c 1 by c 2, where c 1, c 2 are integers. Now take out the even powers of 2 from c 1 powers of 2 from c two. So, I can write this as 2 to the may be m times c 1 prime by c 2 prime, where c 1 prime c 2 prime are odd and n is an integer positive or negative whatever it may be (Refer Time: 41:45) may be.

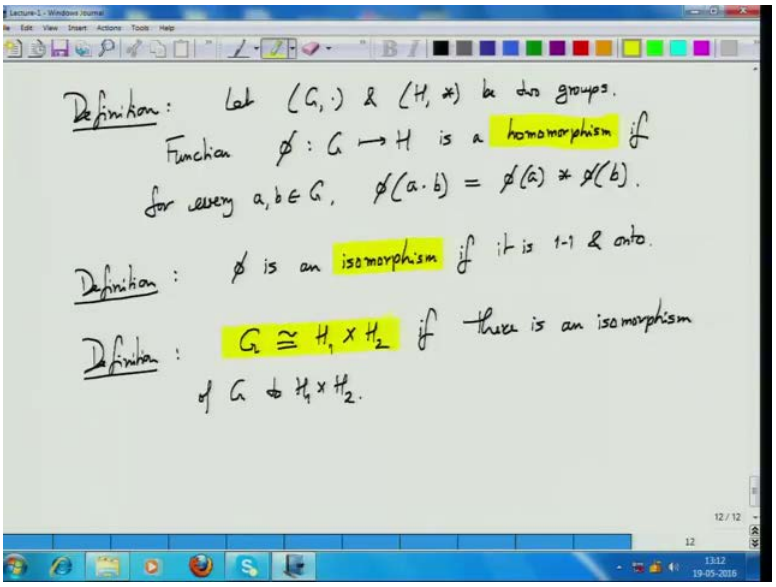
So, this is in 1 to 1 correspondence with 2 to the m comma c 1 prime by c 2 prime see this view allows us to transform a given element of Q star to the corresponding elements of H 1 h cross H 2 and vice versa. If you are given an element of H 1 cross H 2, just multiply their 2 them and you get an element of Q star. If you get an element of Q star, you would do this process of separating out powers of 2 and then that splits as an element of H 1 cross H 2. So, this correspondence I claim is 1 to 1. Do you see that if you have two numbers c, c prime mapping in the same that to the same; that means, they are powers of 2 are the same and the odd component are the same then numbers have to be the same.

Similarly, the reverse way two elements of H 1 cross H 2 map to the same product then since the product have separate powers of 2 and hard part again they will both be the same numbers. So, it is a very simple correspondence, which shows that Q star can be viewed as H 1 cross H 2. One more thing the group operation on Q star, we should also ensure that it is same as the group operation on H 1 cross H 2. Group operation on Q star is the multiplication when you do multiply two numbers of Q star what happens to their powers of 2 present, you multiply the powers of 2 of the two numbers then the odd part also you multiply them, which is exactly what the operation on H 1 cross H 2 is.

So, this demonstrates a complete correspondence between Q star and H 1 cross H 2 and that is the situation when we say that a group like Q star can be factor or returned as a product of two subgroups are you with me so far, yes. So, let us formulize this is just an example to motivate this definition which I am going to give now the key thing is this

correspond, how do we formally state this correspondence between the group and the product H 1 cross H 2 and that is done through the notion of an isomorphism.

(Refer Slide Time: 45:00)



In fact, I will do it in two steps. Let G dot and H star be two groups. We say that a given two groups G and H under their own of group operations in mapping phi taking elements of G to elements of H is a homomorphism. If the following property, while in the property simply says, that the mapping phi respects the group operations. Phi of a dot b, a dot b is a group operation of G phi of that element, which you obtain after well you know doing a dot b is same as phi of a star phi of b star is a group operation under H.

So, it does not matter whether we have first do the group operation in G and then apply phi or first apply phi and then do the group operation H. So, this is also in a way saying that phi preserves the group operation while moving from G to H. Then comes the second definition the in a homomorphism it is not necessary that the mapping phi is a 1 to 1 or onto mapping phi is an isomorphism. If phi happens to be a 1 to 1 and onto mapping from G to H, then it is called an isomorphism.

So, it is a isomorphism is a very special kind of homomorphism and it is the isomorphism that we have been talking about earlier when we say that G can be written as H 1 cross H 2, what I really formally want to say there is a G is isomorphic groups H 1 cross H 2. Because two isomorphic groups are essentially the same groups you can put

elements into 1 1 correspondence and the group operation is preserved whatever is the group operation in one side the group operation on the other side.

So, with these definitions I can now finally, say that that is the next definition I am to finding lot of them. So, this is a notation we will use to represent isomorphism between two groups. We will write an equal to and the till they on top of equal to sign and this designates that the two groups are isomorphic to each other. This is with respect to the previous the product definition that this H 1 cross H 2 as we had defined H 1 H 2 being subgroups. If we can write G as a isomorphic G as isomorphic to H 1 cross H 2, then it gives us something very nice or tells us something very nice about the structure of G. Then I can actually factor G as two subgroups.

Time to stop today, and then we will continue tomorrow.