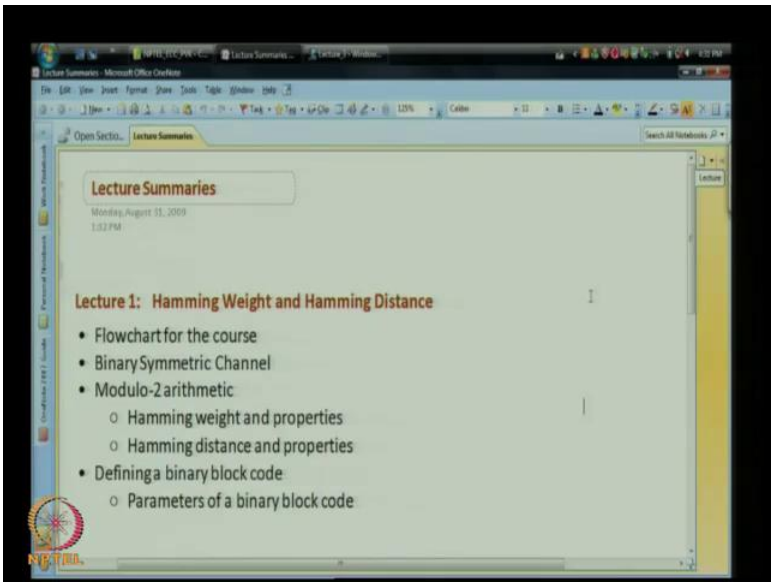
Error Correcting Codes
Prof. Dr. P. Vijay Kumar
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore

Lecture No. # 04
Subgroups & Equivalence Relations

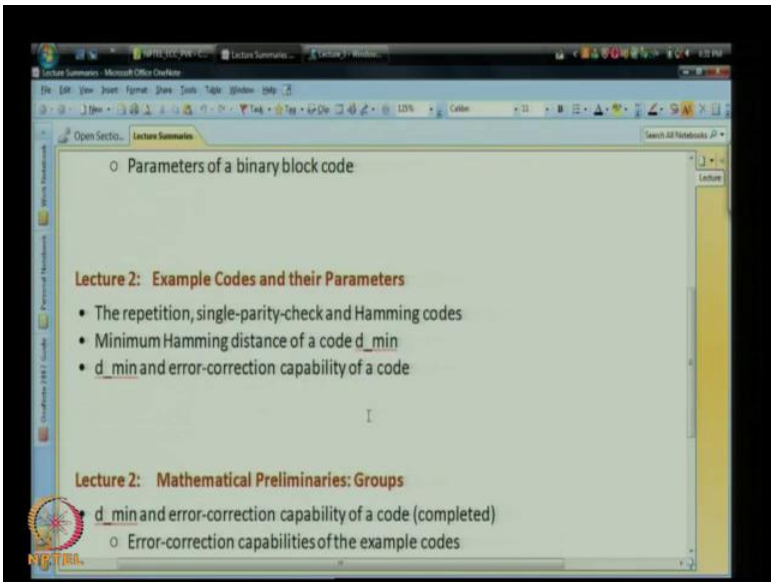
This will be our fourth lecture and the way, I like to begin is by quickly reviewing the material that we covered in the first three lectures; and then will continue, what we were doing in the last lecture.

(Refer Slide Time: 00:32)



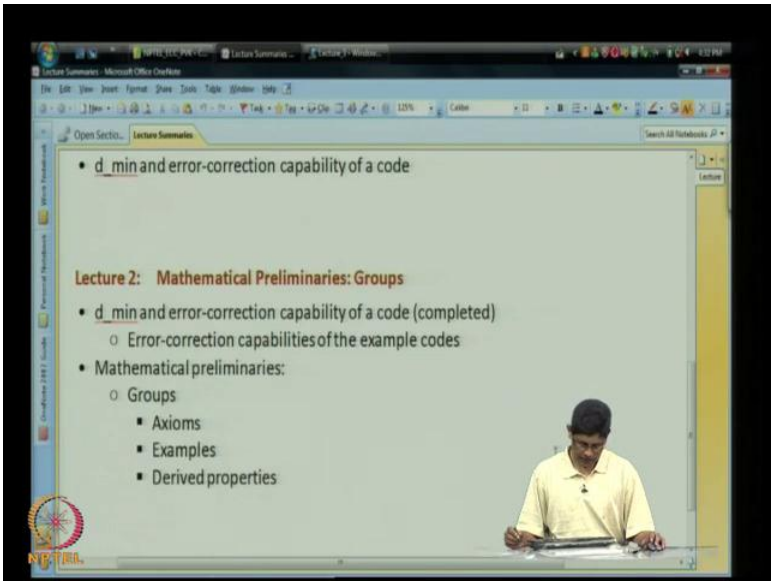
So, if we can go down to the screen here; so here is the summary of what we have done up to now. So, we covered in the first lecture, which I in title hamming weight and hamming distance, we looked at flow chart for the course, we looked at the binary symmetric channel, then we looked at modulo 2 arithmetic; how to work with vectors, whose symbols are binary. We defined, what it means to talk about binary block code, and also the parameters of a block code.

(Refer Slide Time: 01:02)



Then in the second lecture, we looked at example codes and their parameters; the repetition single-parity-check, and hamming codes. We looked at the minimum hamming distance of a code, which is defined to be d min, and then we looked at relationship between minimum distance of code, and its error correction capability.

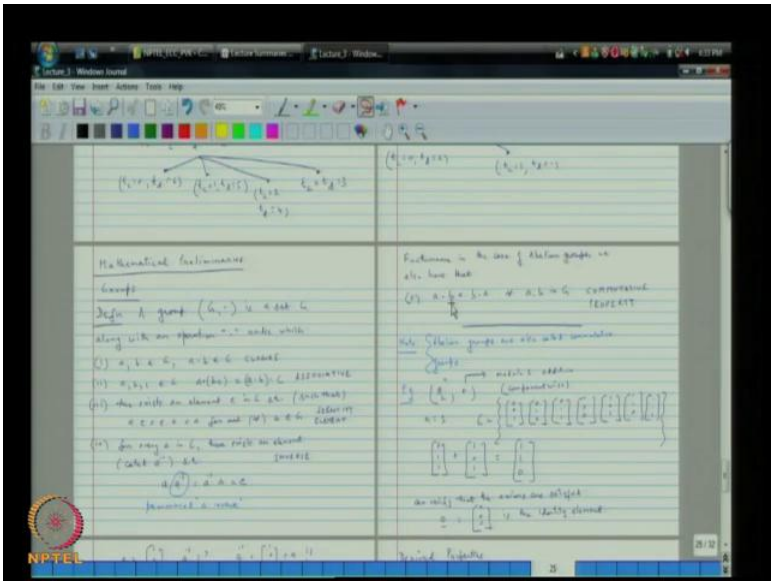
(Refer Slide Time: 01:21)



Then in the last lecture, they should be three; in the last lecture, we talked about mathematical preliminaries, groups. We began by computing earlier group on the relationship between, the minimum distance of code and its error correction capability, and then after that we started talking about groups. Now, these are algebraic structures, and so you will have to be a little bit patient, because it is go to have the algebra behind; that is behind all the theory that will study, so will go through that algebra.

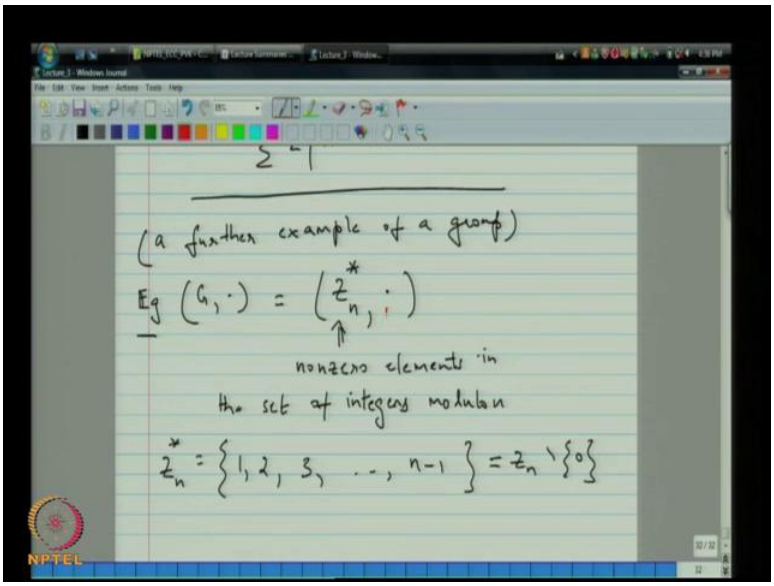
It will take as two or three lectures, and then we will come back to the codes, that will elaborate and progress so much faster. So, getting back to the pad, so we started talking about groups, and we first discussed axioms, that going to be making up a group, will looked at examples and then some derived properties. So today, will continue from there with that I am going to close, this particular file.

(Refer Slide Time: 02:35)



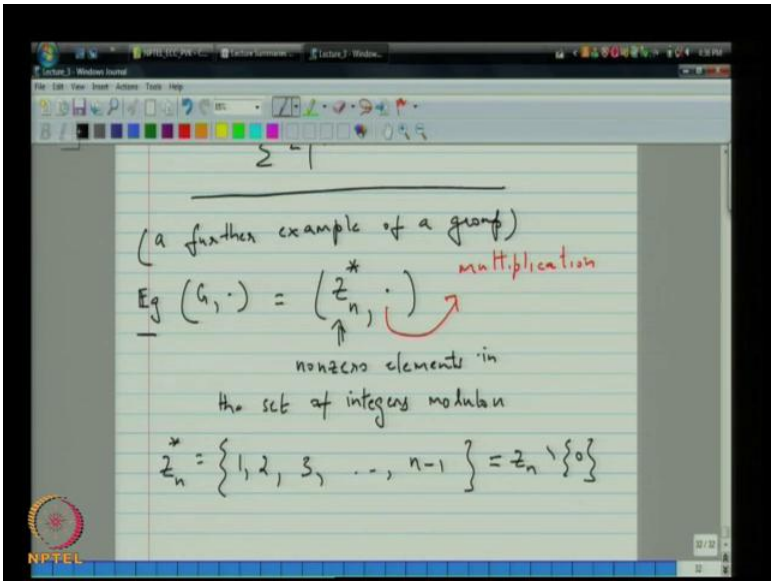
And we will go on to our lecture pad here. So, this lecture pad let me, so quickly remain this. These on the on this side here, you see the axioms that define a group, and then then we looked at some examples, we looked at derived properties. There is properties that followed from axioms, and that is about where we are, so we continue from there. So, this then... I will title this lecture, as sub groups and equivalence relations, but first continuing on from where we had left of last time, I like to discuss one further example.

(Refer Slide Time: 04:22)



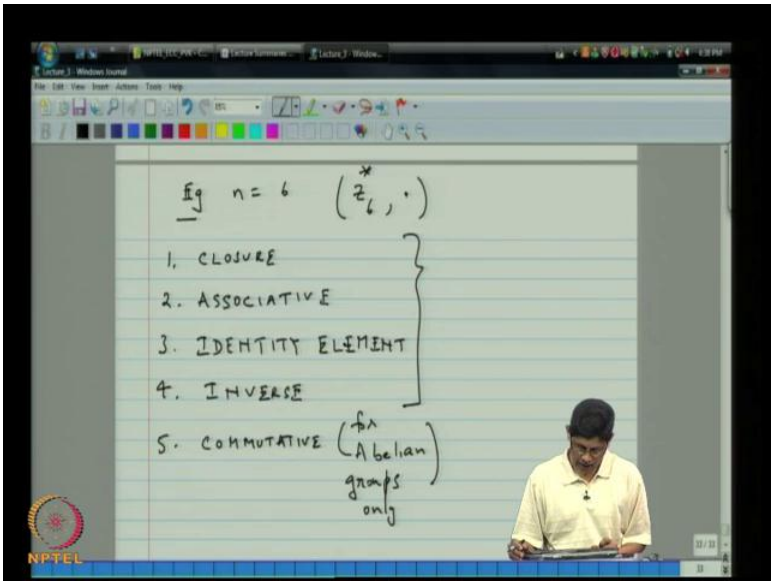
So, further example of a group. This is the case, when we are looking at the group and operation is z sub n, and I put a star on top and this. So, first of all, with regard to the notation, this think here is the non-zero, the set of nonzero elements, in the set of integers, modulo n. So you can z plus as precisely the set 1, 2, 3 all the way up to n minus 1. So, exclude in other words this is z set n that with zero element remote.

(Refer Slide Time: 05:53)



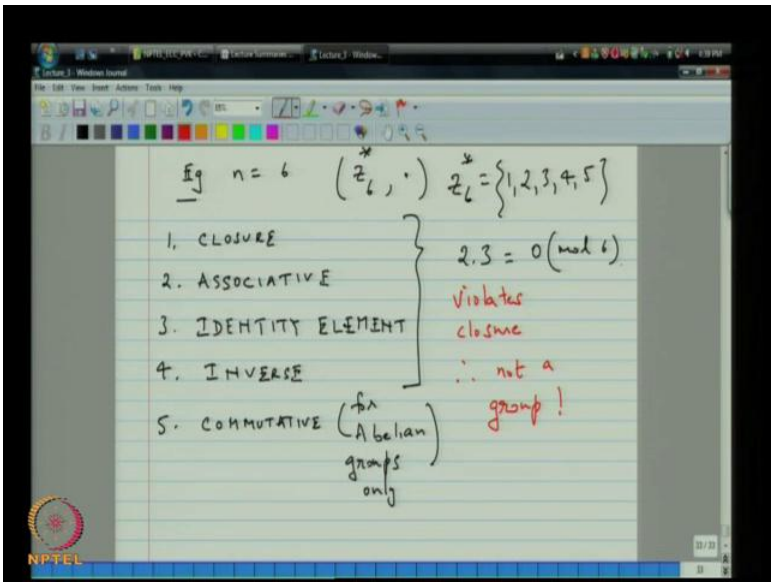
And here, this thinks here this operation is multiplication. So, earlier we have looked at addition and this time going to look at multiplication is our operation. Of course, one question is, what is n right? So, n is an integer, so we look at an example within an example.

(Refer Slide Time: 06:22)



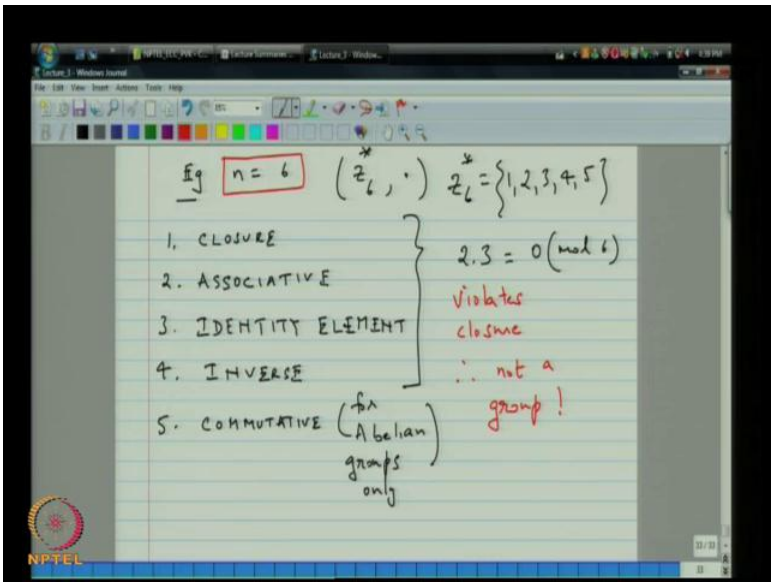
So, let us say we look at the case, when n is equal to 6, so we are looking at z 6 star and multiplication, and the question is thus this form a group. The recall, that in order first something be a group, it have to a satisfied following axioms. 1, it has to satisfy axiom of closure. 2, the multiplication (( )) had to be associative. Then you needed the presence of an identity element, you needed the presence of inverse, and in the case of an abelian group, you needed that it be commutative.

(Refer Slide Time: 08:00)



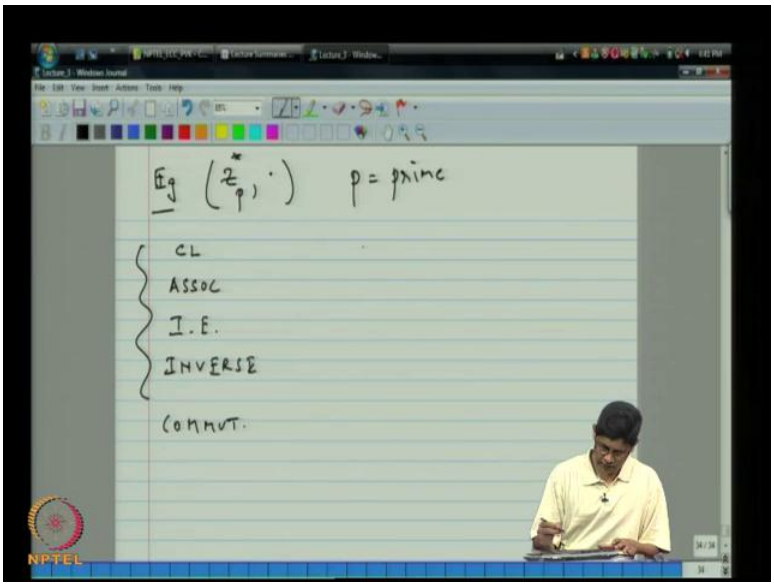
So, basically therefore operation that you need to check, and so right away, when you look at... Of course, z 6 star is this set; it is 1, 2, 3, 4, 5, and 0 is excluded. Right away you see that if you multiply 2 by 3, this is 0 modulo 6 and that is a problem. Because now, we are multiplying two elements in the set, but what your getting is an element (( )) this set. So, the closure requirement is validated, so this violates closure. The conclusion is that this is not a group, therefore not a group. Now if, you look at this proof in say, why is it, that this group failed. Well the proof failed.

(Refer Slide Time: 09:03)



Because we choose, we started of with n equal to 6. Now, 6 is the product of two integers. So, that since to say that may be choose integer n which is not divisible. Then perhaps this some hope that this violates could not occur, so will look at a slightly defined example.

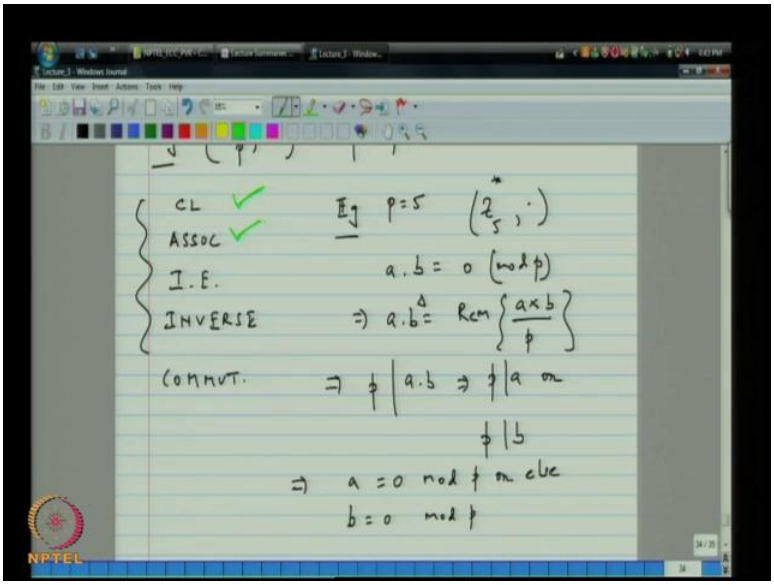
(Refer Slide Time: 09:32)



So now, we look at z p star and multiplication, for this time p is a prime. Now, it is typical in algebra, to serve p or q to the prime. So, in this case then integer n is replaced by prime p and

again, we have to check for the following axiom. You have to check for closure associative property, the presence of an identity element, the inverse and whether it is commutated. If, you want to be abelian group this time, you can check that for us closure concerned. So, if you take, since I do not want this, to be a formal proof, I just want to convey be idea to you.

(Refer Slide Time: 10:43)

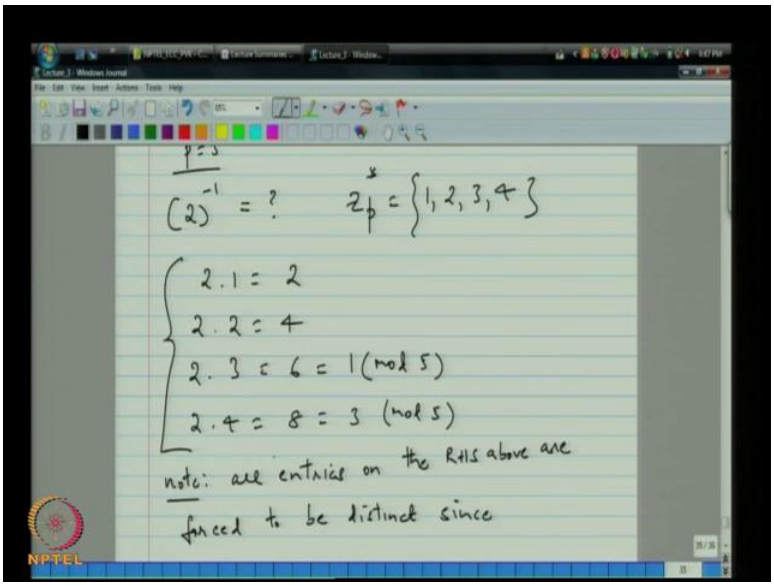


So, let us take an example when p is 5, so it is an example within an example. z 5 star with dot and other question is if multiplication, is it closed. So, is it possible? That a into b is 0, mod p without either a or b being 0 mod p. But this is clearly impossible. Because saying this, because when you say a in to b, what you really mean, is the remainder. When you multiply a times b and divide by p. This is how you defined it. Let be put down multiplication here. So, it is, this is ordinary multiplication.

That is, what you really mean, when you write down a times b? If, the product is zero mod p, that means there is no remainder, which means p divide a times b. So, a times b equal to 0 implies that p divides a b. But you know that p can divide a product to a integers if, only if p divides either one of the other of them or both, but that means that implies a equal to zero mod p or else or else b equal to 0 mod p. So therefore, what we found is that a times b equal to 0 cannot happen, because a and b or in z p star. So, the conclusion here is that closure is satisfied is no

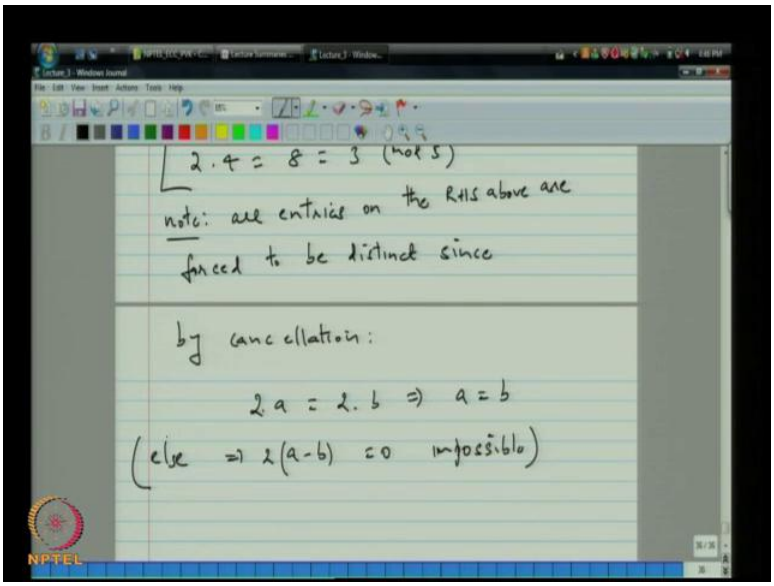
problem. There, we can similarly check that the associative property is satisfied, and also the identity element is just to one. So, that leaves of the question of inverse.

(Refer Slide Time: 13:16)



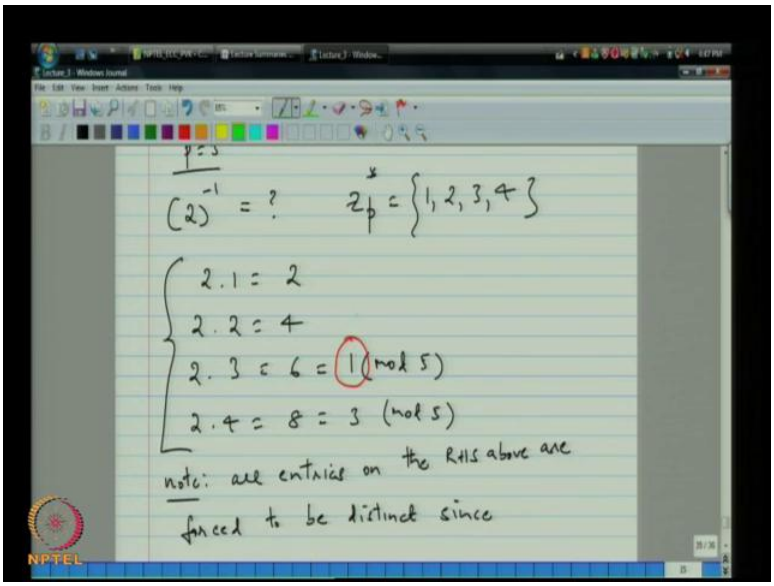
Perhaps, what the inverse let us look at the inverse. So, again let us look at the case from p equal to 5 and supposing, we want to know, what is the inverse of 2? So, what we can do is we know that z p star consist of 1, 2, 3, 4. So, we take two and multiply all these elements limited. So, 2 into 1 is equal to 2. 2 into 2 is equal to 4. 2 into 3 is equal to 6, which is 1 mod 5 and 2 into 4 is 8, which is 3 mod 5. Now, as you look at this you notice that all, all the results on the right hand side here or different and in fact they have to be... Because note all entries on the right hand side above are forced to be distinct.

(Refer Slide Time: 15:05)



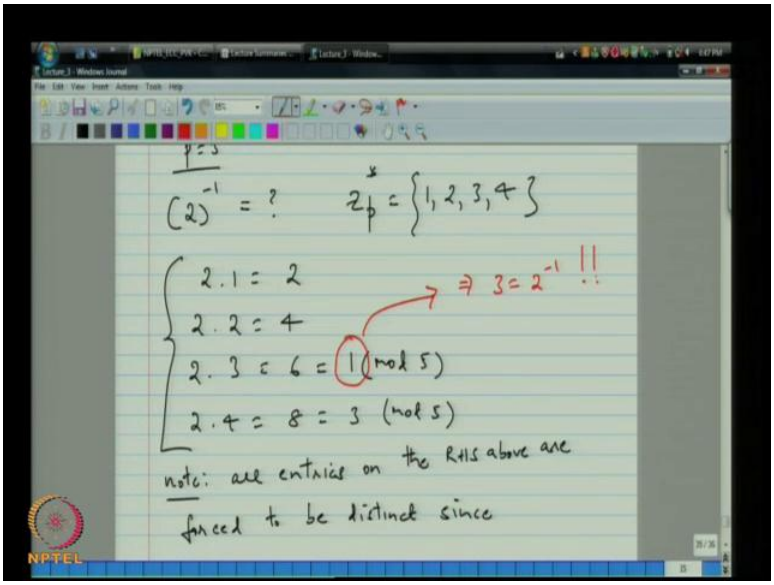
Since by cancellation, 2 into a is equal to 2 into b implies that, a is equal to b, because otherwise else this would be imply, that 2 into a minus b equal to 0 which is impossible. So, again let me repeat, so we are now, looking at z p star, when p is a prime; in particular, when p equal to 5, and we want to check whether, the axioms to the group hold. So, we already check closure the associative property, and the presence of an identity element. The identity element is equal to 1, this nothing much there, how about inverse? That is the question, we are trying to inverse here and I am going to illustrate, the general proof, by looking at the example, when p is equal to 5. Supposing we trying to look at 2 inverse now, defined 2 inverse, what you can do is, you can multiply two by all the non-zero elements in here. In separation and it has to be either all the elements on right hand side will be distinct, which means that all these elements must appear on right hand side exactly ones.

(Refer Slide Time: 16:41)



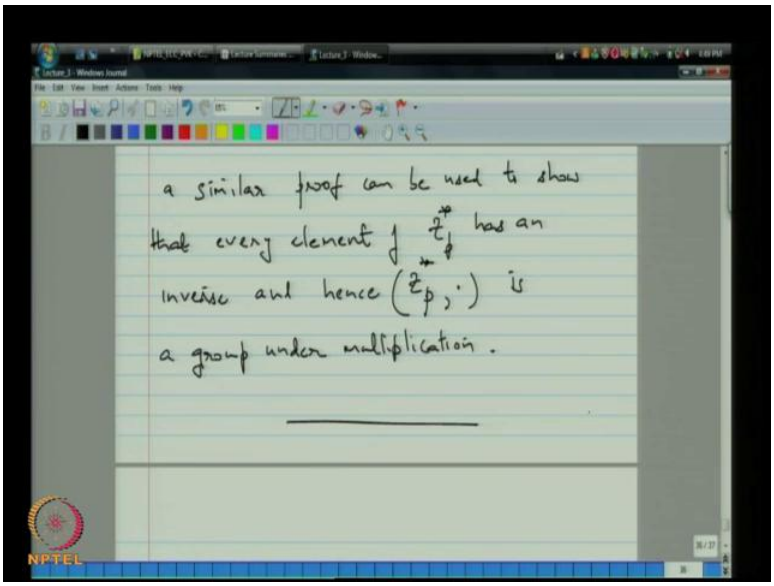
That in particular what there actually means is that, even 1 will occur exactly ones. So, that means that, there some elements as 2 in to 3 is 1. Now, that means that, 3 is actually 2 inverse. This group is, by the way is commutative, this group is commutative, so far the inverse only need to check, that I get one can multiply on right hand side.

(Refer Slide Time: 17:00)



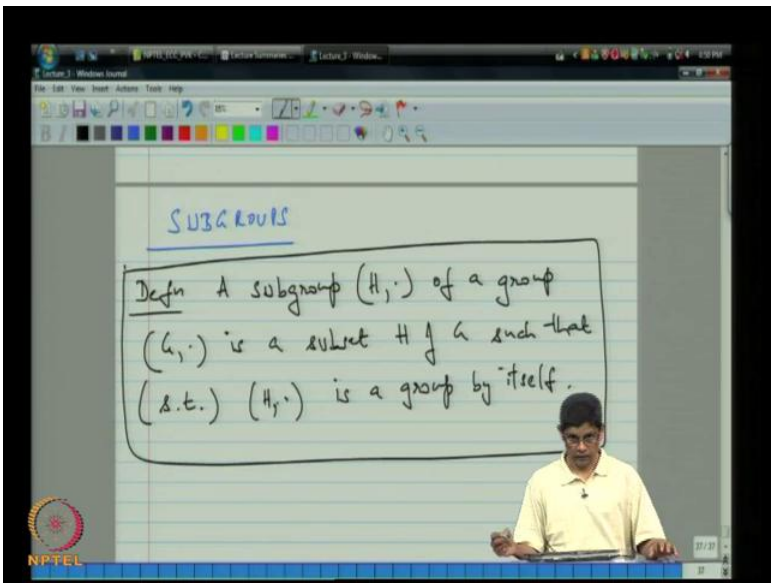
So, what this actually implies this implies that 3 is 2 inverse. In general, this proof can be extended to show that inverse exist in general.

(Refer Slide Time: 17:34)



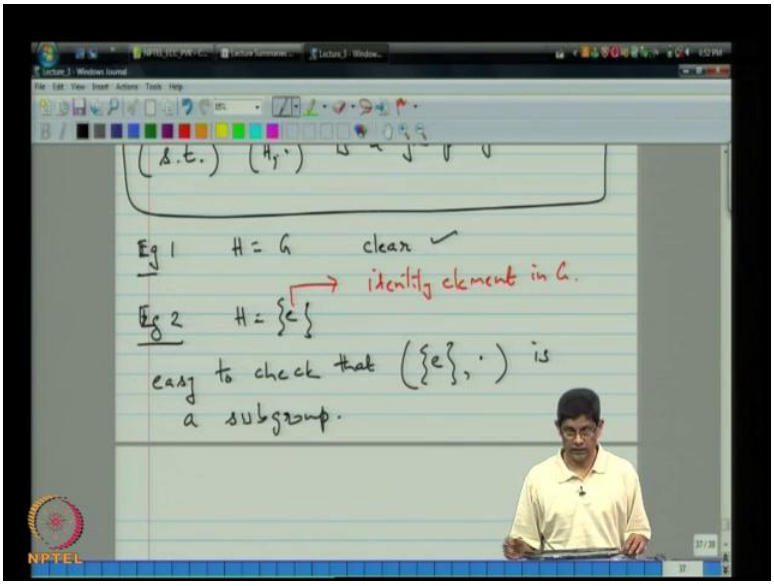
So, similar a similar proof can be used, to show that every element of z p star has an inverse, and hence z p star is a group, is a group under multiplication. That concludes yet, another example, of a group and now what I like to do is continue by talking about subgroups.

(Refer Slide Time: 18:53)



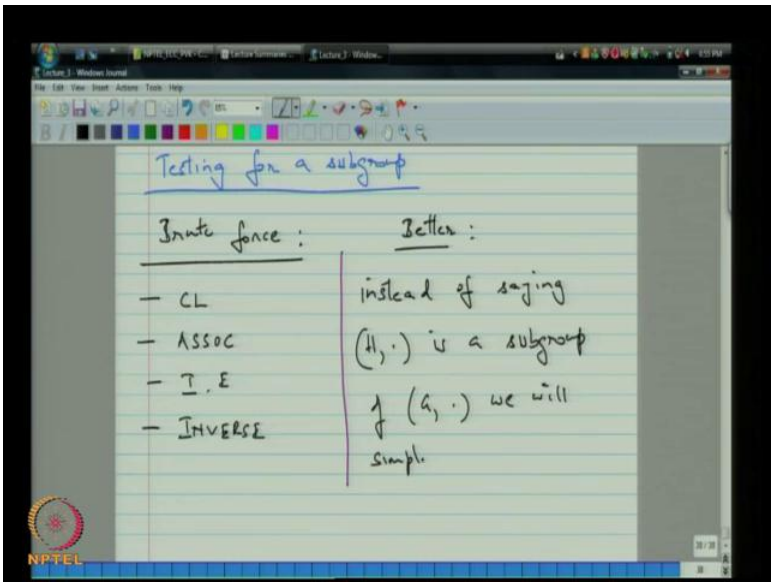
So, will begin with the definition, a subgroup H dot of a group G dot is a subset H of G such that (( )) abbreviate such that there writing s dot t dot, such that, H is a group by itself. So, that is the definition of sub group.

(Refer Slide Time: 20:23)



Let us look at an examples, the the first two examples of trivial examples. H is equal to just the group itself, that is clear; it is clearly subgroup. The second example is the case when each is a set that consist of only the identity element of G. Here e is the identity element in G and you can verify that this forms a group. I just either is easy to check easy to check that is a subgroup. These two examples, the two extreme cases, when the subset H of G is all of a group and the subset H of G is just single element these are ah the two extreme. These are called trivial examples.

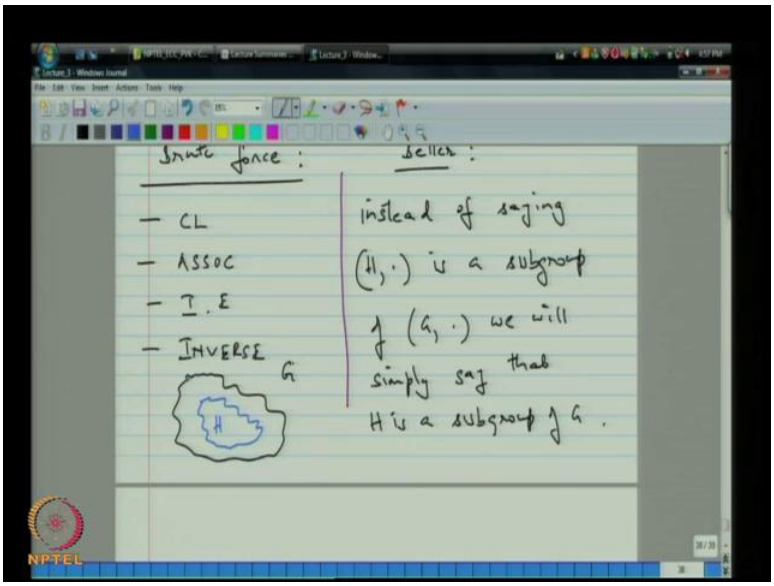
(Refer Slide Time: 21:57)



Now, we will look at couple of other examples, that before that let us get in two, in other issue, which is how do you test for a subgroup? Now, this brute force way, the brute forced method. It check following, it will check to make sure that closure. Associative property, the identity element and the inverse, all exist. But this clever all method. If, doing it this a better method and that is to make use of a lemma to actually put this down is lemma one, let me before I do that perhaps should make one clarification, instead of saying H plus is a subgroup of G plus, we will simply say that H is a subgroup of G.

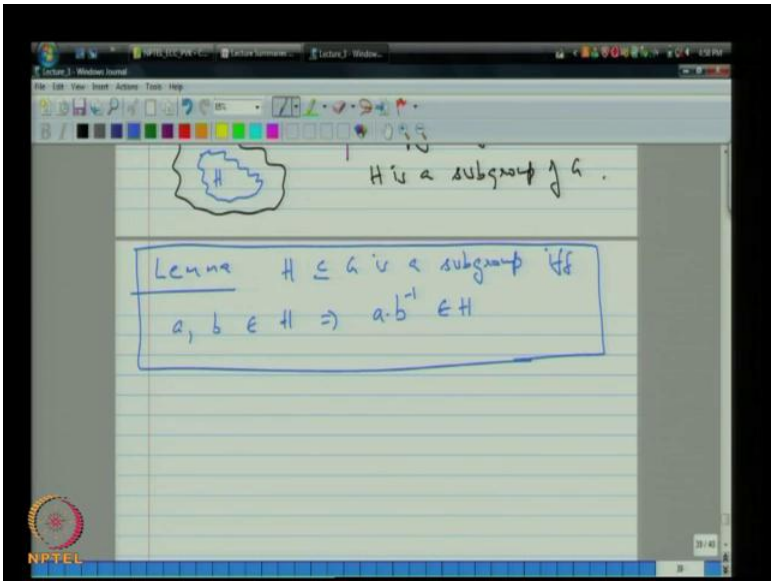
I mean, it is just is a short form. Strictly, speaking when you talk about a subgroup, what you really mean is, that there is a group, there is a set and there is a group and then you are talking about subgroup. You looking at a subset of that is main set, universal set and then we looking at same operation in you are trying to show that is a group. So, strictly speaking should talk about, going down to the pad, we should talk about H dot as a subgroup of G dot, but that is too cumbersome, so will say just simply, that each of the sub group of G. Here is lemma, so the brute force way is to actually looking to each and I may be actually draw small picture here.

(Refer Slide Time: 25:33)



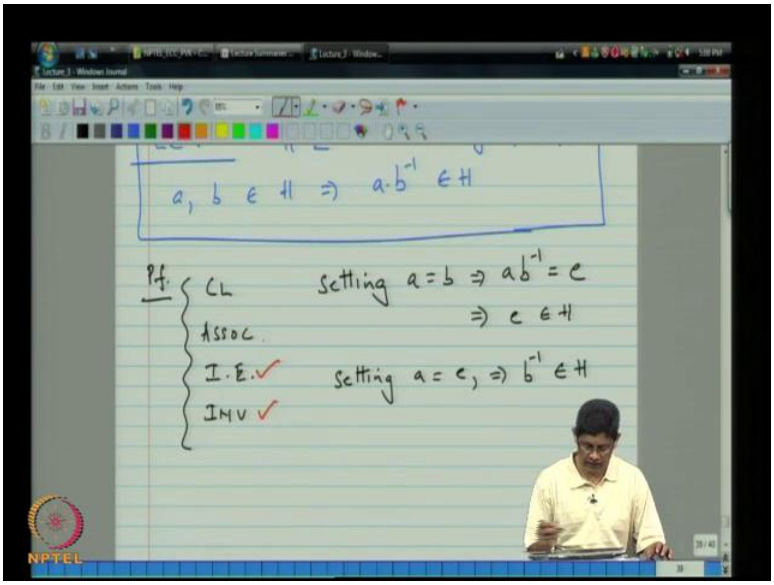
So, here is a picture that is you have here group G and hence sitting inside this, you have subset H and what you want do is test, whether the elements in this subset actually form a group and the same operation. So, brute force way is to test apply the entire force test, but that a way, but simpler method is to apply the following lemma.

(Refer Slide Time: 26:20)



Which says that, H subset of G is a subgroup? If and only if a, b in H implies that implies that a times b inverse, belongs to H. So, it is a simple test. In some sense, you reduced the requirement of checking four thinks. You just checking simple item and will see, there is a better useful when we come down to checking, whether something is linear code or not so that is an application here. So, let us go head in proof this, so the proof.

(Refer Slide Time: 27:24)



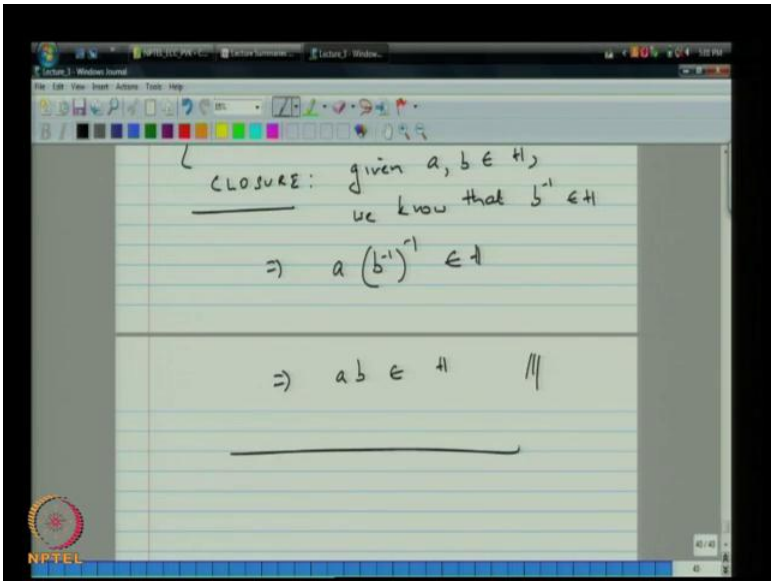
Now, again let us keep in mind that we need to sure, that this single test is a substitute is a valid substitute for the for the axioms, which are the axioms of closure, associatively the identity element and inverse. Now, as far as closure, so let us we want to (( )) them that order, it is convenient to actually tackle the identity element first. So, when we set setting a equal to b implies that setting a equal to b, implies that ab inverse is equal to the identity which implies the identity element belongs to H. Thus, we will check that the identity element belongs. Next, setting setting a equal to identity, because now that we know it is there tells us that b inverse belongs to H.

So, that gives us that the inverse is also there. Now, the associative property something that we did not have to test for; the reason being that if you think about it. I mean there is a property of associability with respect to multiplication, remember that the associative property requires that

the way in which group elements to gather before multiplying does not matter. So, since that holds, for pairing group it also holds for a subset. So, we do not earlier to test for that.

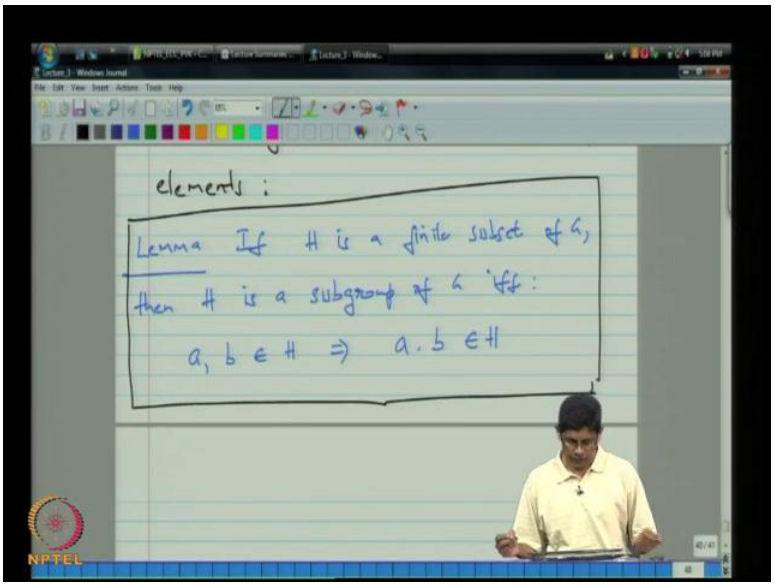
So, I am just going to without any further argument, will just put down it take for that. So now, we come down to the question of closure. So, closure means, that given that a and b are in a b in H, that in a times b in H.

(Refer Slide Time: 30:10)



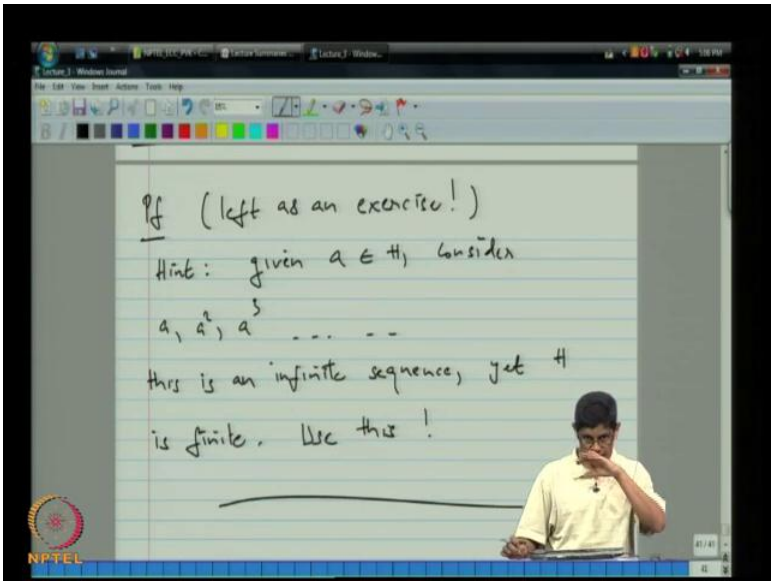
So, for closure, given a b in H, we know that, b inverse belongs to H, which implies that, a times b inverse inverse belongs to H, which of course implies that, a times b belongs to H and we have done. That is are you take care of closure, because the inverse of the inverse is the element itself as you can check. That finishes that proof. Now, in summary if, you want to check something is subgroup, you just imply that one test from now, one there is a further simplification in the case of in the case of groups that have a finite number of elements.

(Refer Slide Time: 32:17)



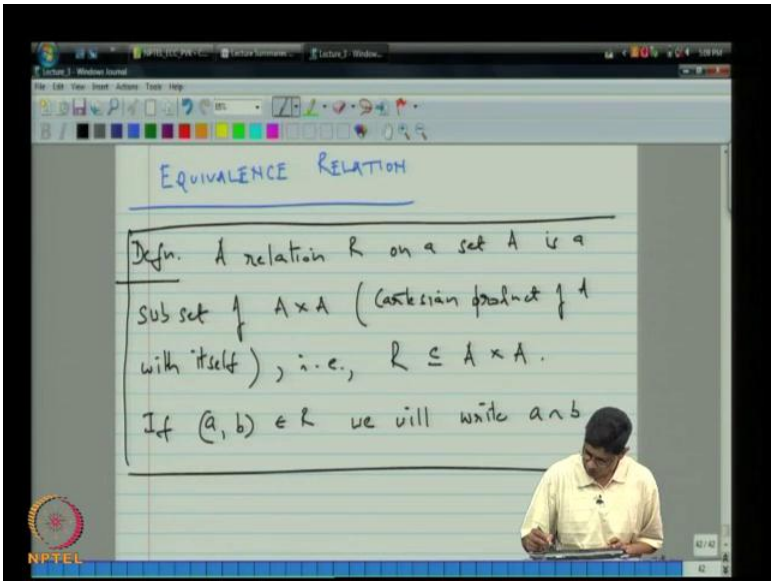
Will put down lemma, for that if, H is a finite subset of G then H is a subgroup of G. If, and only if a b in H implies that a time b is in H or in other words or in other words in particular case of finite subsets, it is sufficient to just check closure. Now, in the interest of moving along, I will not proof this. I move you to proof this in an exercise and apart as a hint, I just asking to consider given a in H.

(Refer Slide Time: 34:00)



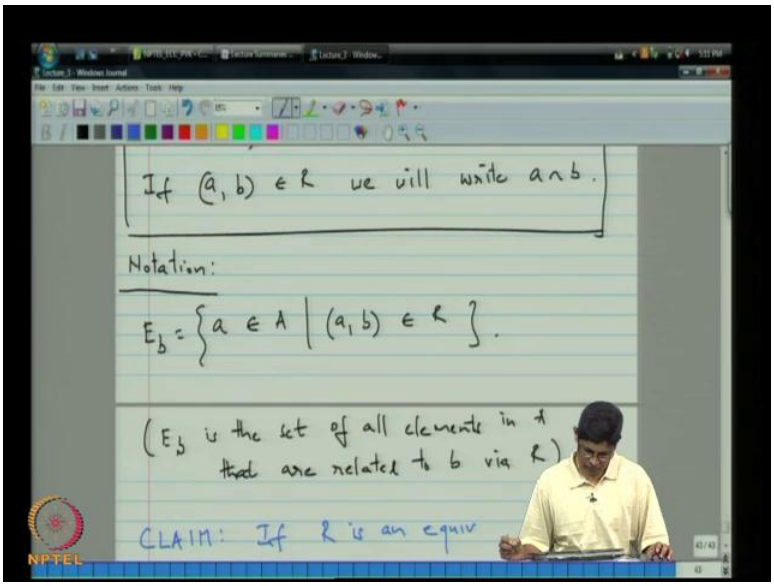
Consider a, a square, a cube and so on. This is a, this is an infinite sequence. Some infinite sequence, yet H is finite, use this. You might enjoy trying, that out you are on. So, basically you look at this sequence a, a square, a cube and so on which goes on to infinity, but all the elements are belongs to H. Because we need to H on property, there if a b belongs to H and a times, b belongs H. So, in particular if, a is equal to b then a squared belongs a cube belongs, a to the four belongs and so on. This is an infinite sequence and but under (( )) a should finite must really, it is finite. Use that property, in other words there, must be some repetitions in the sequence and you should may be used that. Now, we are going to move on to the topic of course it.

(Refer Slide Time: 35:52)



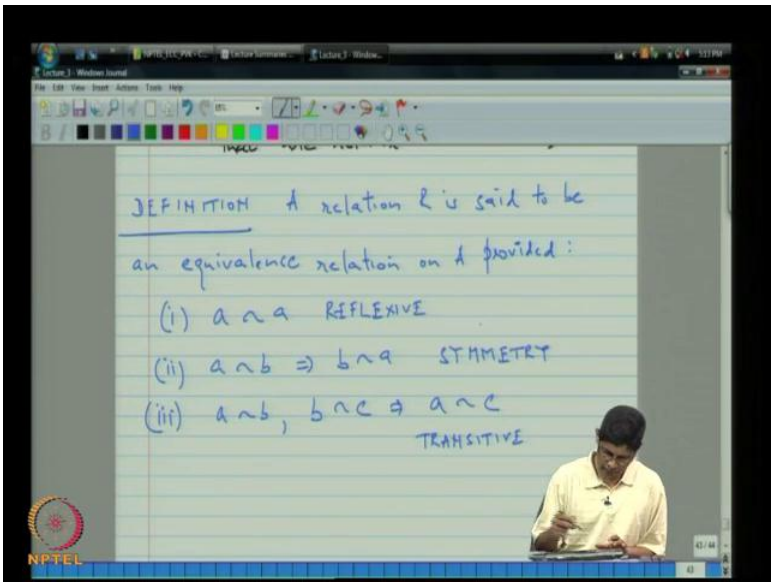
We will begin with the motion of equivalence relation. A relation R on a set A is a subset of A cross A. This is also called the Cartesian product of A with itself, so the Cartesian product simply means, that you just take all pairs a b, where a comes from a and b comes from a. i e R is a subset of A cross A. If a, b is in R which means that a and b are related by relation R, we will write we will write a equivalent b. Let me at the same time introduce some other notation.

(Refer Slide Time: 38:00)



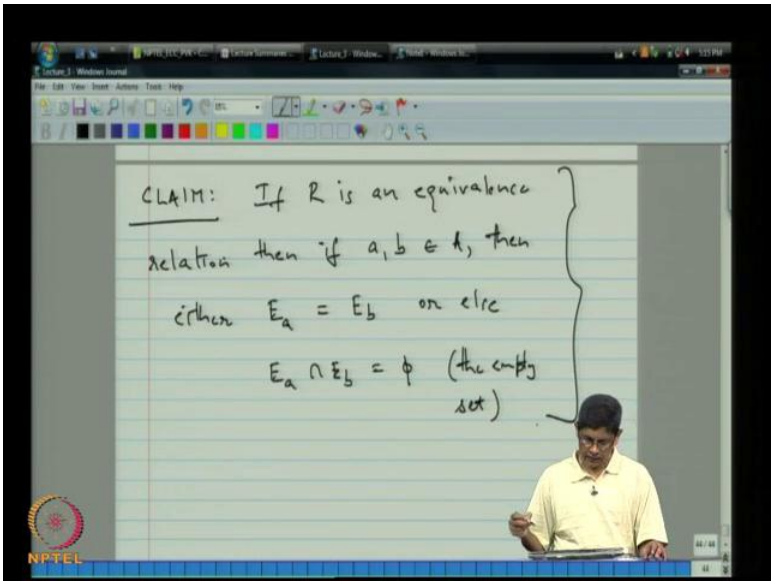
The notation is that, E b is the set of a in A, such that (a, b) belongs to R. So, in other words, is the b is the set of all elements a, which are related to b through relation r. So, loosely speaking E b is the set of all elements in A that are related to be via, relation R. Now, I claim the following if, f R is an equivalence relation r, let me just back track I think head of myself here, before I can make this claim, I just going to make a claim about this property of this set b, but I need to introduce other notation first. So, let me just erase this that track will come back to this point ok this one other point there I need to take here of... So, within the clause of relations there is clause of relation that is called known as equivalence relation. This satisfies certain additional properties.

(Refer Slide Time: 41:00)



A relation R is said to be an equivalence relation, on a provided, that all this conditions following relations are satisfied. We need to one, that a is equivalent to a, this is called there reflexive property. Two, a equivalent to b, implies that b equivalent to a. This is called the symmetric property .The third property, is that if, a equivalent to b and b is equivalent to c, this implies that a is equivalent to c and this is called as the transitive property. We look at some examples very soon. So, now we ready to make a claim that I had stated as earlier.

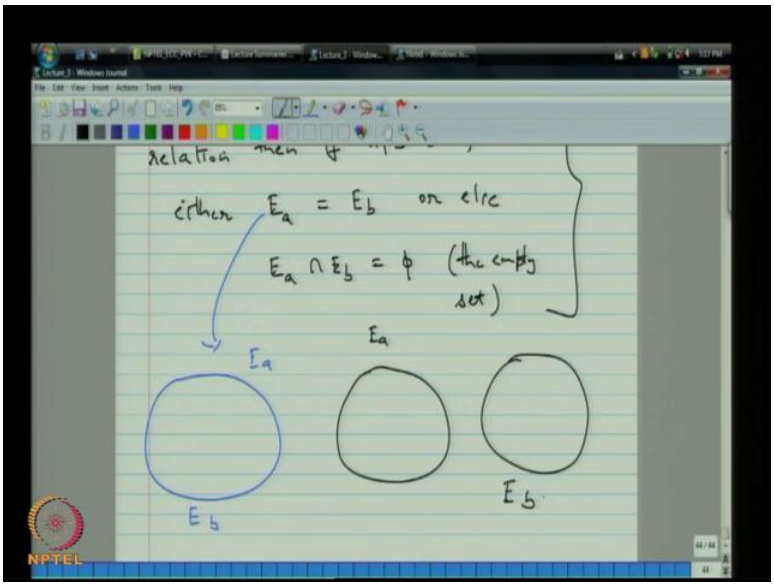
(Refer Slide Time: 43:13)



Claim if, R is an equivalence relation then if, a b belong to a then time either, E a is equal to E b or else E a intersect E b is the empty set. This is, this is like all are in nothing property. Let me just try to make that picture here, we first defined a relation on a sector, we said relation means ah subset of a cross R.

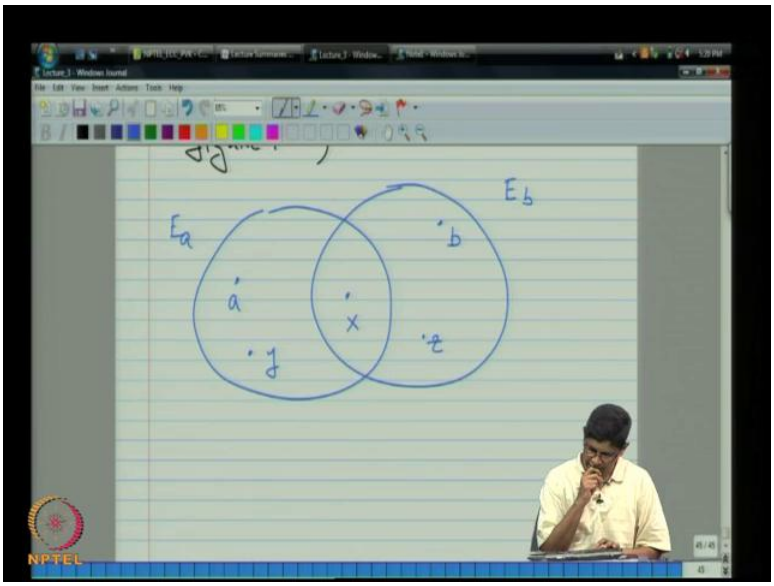
So, just pairs we just fix certain pair, they are related or relation R. However when the relation had certain properties mean that if a is related to b then b is related to a, must be related to itself. If, a and b are related, then a and c are related. If the relationship of this type, this is the type that will be interested in encoding theory, then it said to be, an equivalence relation, this is said to be an equivalence relation. If, R is an equivalence relation, an if, a and b belong to a then either a equal a b or else a intersect a b is the empty set.

(Refer Slide Time: 45:54)



So, that means that there are only two possible pictures that you can have in mind. So, one of themselves, that the pictures like, this you have E a, and we have E b and there then in the same or the other property else. So, the other property is that either have E a like this and E b like this. Either be sure all elements in common or nothing and its really equal to easy to see why this must be the case.

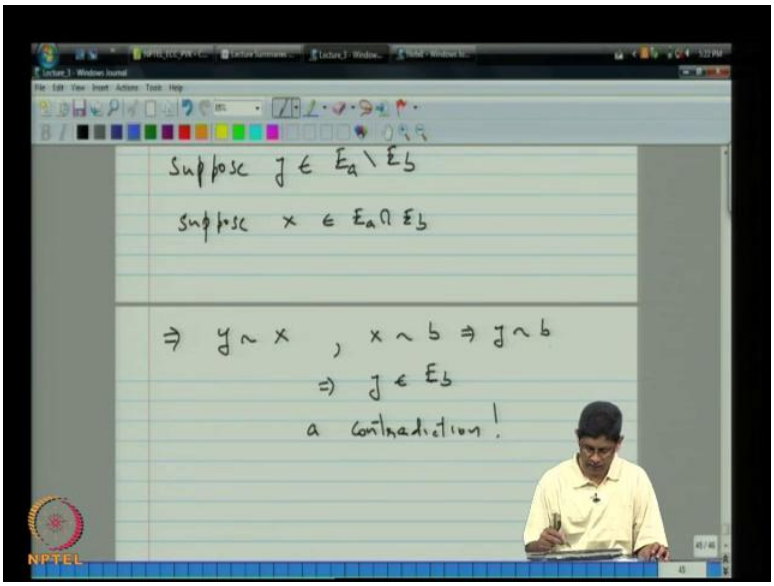
(Refer Slide Time: 46:34)



We will sketch that the proof using a figure, and the figure basically this. Let say, that suppose the situation was like this, supposing there was an element, x that belong to both E a and E b. Now, this is the equivalence clause of a. So, certainly by the reflective property a belongs here and we know that b belong here. So, what this figures using this, just is it possible that, they can have some elements in common without being the same. These are elements in common.

Now, certainly if they, are not same must be some element, some pair of elements, which do not belong to the intersection. So, let say a and b may or may not belong to that intersection, I am not going to use them. But let us pick two other elements, you pick two other elements; let say will call this y and z. There are since if a is not (( )) a b this must be the case. I am right, but we know actually, I just I do not really mean the presence of two elements here.

(Refer Slide Time: 50:39)



Just one will do supposing this two element y, which does not belong to their intersection. So, you need to clarify that writing that down suppose y belongs to E a, but not to E b. And has suppose and suppose x belongs to E a intersect E b, but then this implies, that y is equivalent to x and have x is equivalent to b implies that y equivalent to b implies that y belongs to E b which is the contradiction.

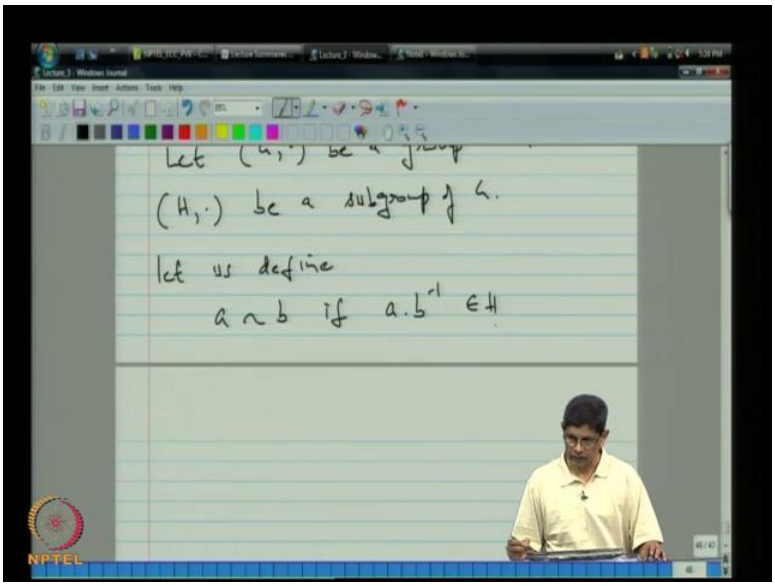
So, let me just run through that again. So, let us say, we have worried following picture exist. In fact, to make things clear let me remove this z. I just pointed out was not needed. So, let us get it trade of result, now supposing this element y which belongs to E a, but not to E b. And we know however that there is something in the intersection in call that x. So, x belongs to the intersection, but this figure tells you that y and x are related , but b and x also related.

y is equivalent to x. x is equivalent to b and other transitive property that means, y is equivalent to b that means that y belongs to E b that is the contradiction, because we assume there is belongs to E a not E b. What is this contradiction, it contradicts the possibility that, it contradicts possibility that, one there is an intersection between E a and E b.

That there is an element y in E a, which is not E b, the only possibilities there exist or either it is something an intersection completely, the same or else begin with they have nothing in common there is such an element, does not exist. So, as was said that sketch of proof you can actually

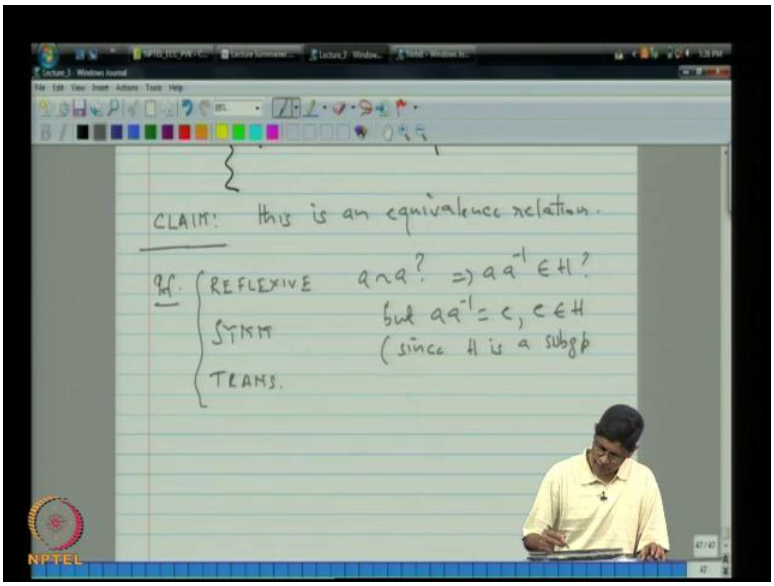
filling the details on your on. Now, I want to talk about type of equivalence relationship, which is useful in coding theory.

(Refer Slide Time: 51:59)



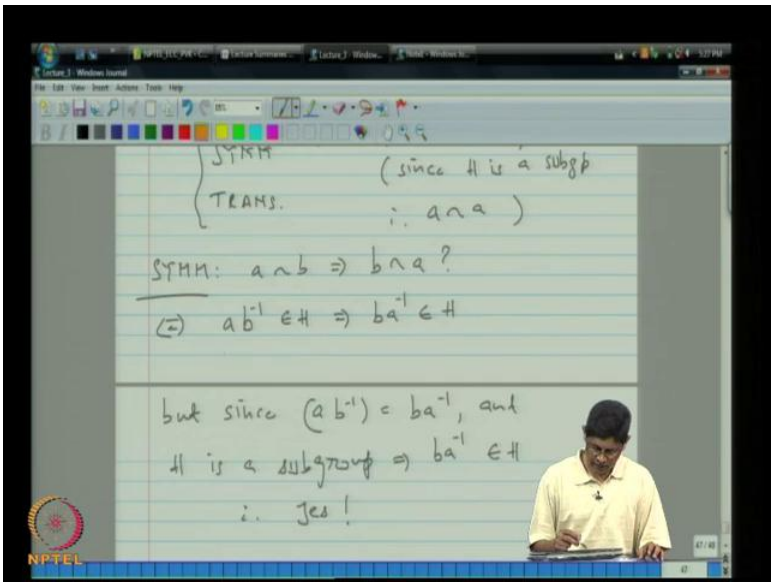
So, cossets of a subgroup let G, be a group and H dot be a subgroup of G. Let us defined, a equivalent b, if a times b inverse belongs to H, now or in other words. i e R is the set of all pairs a, b in G cross G such that a times b inverse belongs to H. Now, what I would to like to convenes, you is that this that this is an equivalence relation. So claim, this is an equivalence relation right proof now, we have to show the reflexive.

(Refer Slide Time: 54:47)



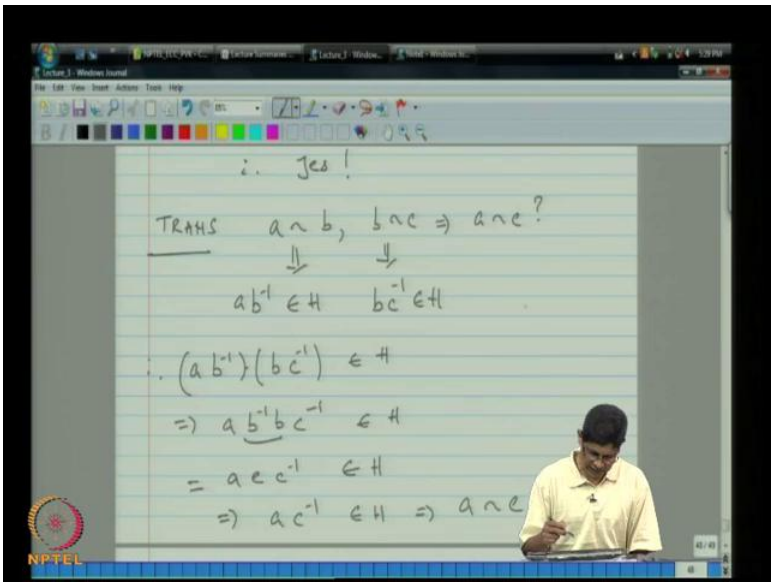
The symmetry and the transitive properties hold. Is a equivalent to a that same assign that a times a inverse belongs to H, that is true because but that a times a inverse is equal to E and E belongs to, since H is a subgroup. Therefore, a is equivalent to a, we shown that the reflexive property is true, how about the others. The symmetry property if, excuse me the symmetry property. If, a is equivalent to b this implies b equivalent to a. So, that is the same as asking the question a b inverse in H that this, implied b a inverse belongs to H, that this is true, but since, a b inverse is b a inverse and H is a subgroup. This implies that, b a inverse belongs to H.

(Refer Slide Time: 56:17)



Therefore, yes the symmetric property holds right. So, we verified the reflexive, the symmetry and the transitive property when to establish symmetry, we have to show a b inverse in H implies, in b a inverse in H, but since that this is just inverse of this if, belongs this inverse also belongs. So, this now problem there, so that gives us the transitive property. The transitive property, as if a is equivalent to b and b is equivalent to c, that this implies that a equivalent to c, but a is equivalent to b is equivalent to saying that a b inverse, belongs to H.

(Refer Slide Time: 57:47)



b c inverse belongs to H therefore, a b inverse times b c inverse belongs to H. Since, it is subgroup, which implies that a times b inverse, b c inverse belongs to H, that this is a identity this middle term is identity. This imply that, a c inverse belongs to H that means, that a equivalent to c. So, where actually proved, what we want to do actually proof. So, all three properties are actually satisfied.

So, will put it tick not this one is as and so we will establish, that this is an equivalence relation right. So, I think that there are closed to when we have obtain. I think this is a good place to stop, apart I just quickly recap, what we did today was, we will continue our discussion an mathematical preliminaries.

We started out in the last class by talking about groups, and today we talk about subgroups, and relations. Before, I am trying subgroup, we talk briefly about further examples of a group. So, in the next class, what will do is will continue further this examples of equivalence relationship, and introduce the motion of cossets of a subgroup. So, with that I leave you, so will captured this again, and then next class. Thank you.