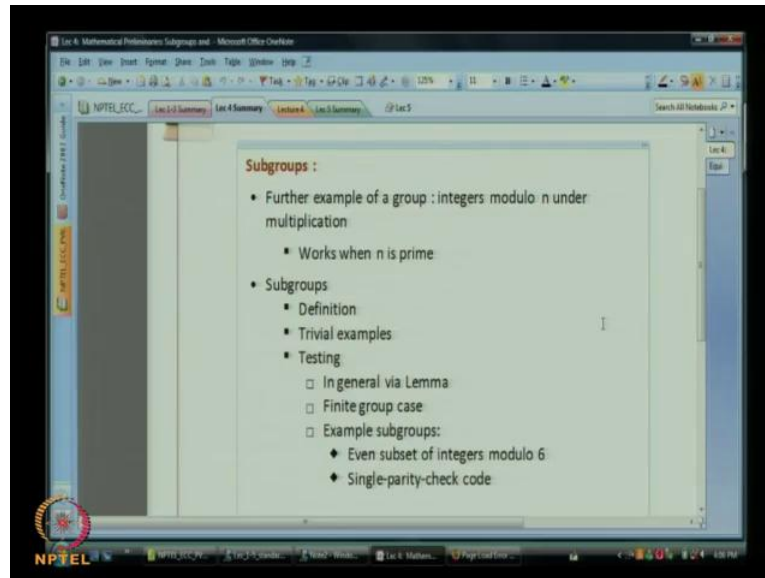


Error Correcting Codes
Prof. Dr. P Vijay Kumar
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore

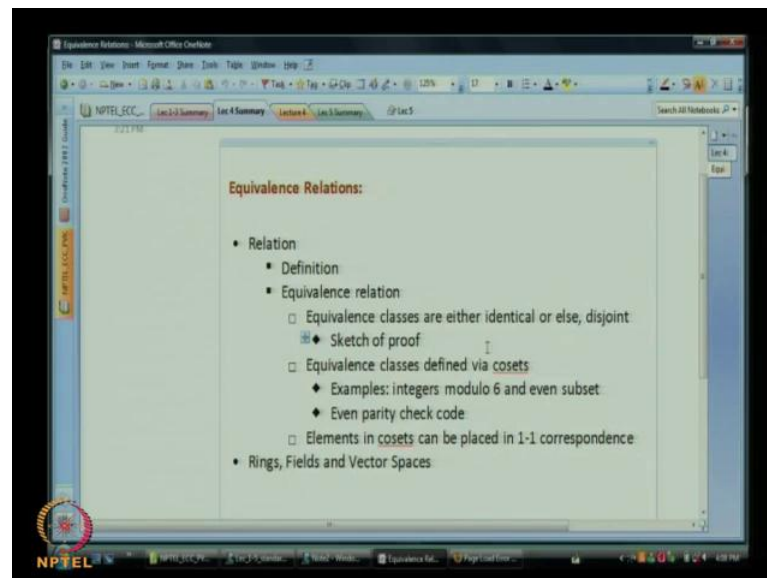
Lecture No. # 05
Cosets, Rings & Fields

(Refer Slide Time: 00:54)



Good afternoon; so, today we will begin the fifth lecture in the series. And let me just begin by going over, what we covered in the last class. So, if we go down to the pad and then I will quickly go over a summary of what we covered in the last class. So, in the last class, we talked about, we discussed subgroups. Before I continued my discussion on subgroups, I gave you a further example of group, that is the integers and modulo n under multiplication. We saw that forms a group the non-zero integers, when n is a prime; so that was our last example of a group. And we went on to subgroups remember, subgroup is a subset of a group, which forms a group on its own under the same operation.

(Refer Slide Time: 02:20)



So, we are provided that definition, and after the definition, we went on to talking about the trivial cases of a subgroup. Then we talked about, how do you test for the presence of a subgroup, without actually going through all the axioms to the group itself. We came with the simple test, and then we simplified this further, for the case of finite groups. We looked at some examples subgroups. The set, the subset of integers modulo six that are even, and also this single parity check code; we saw the both of these are examples of subgroups. Then the next topic that we went on to talk about was equivalence relations. And on the topic of equivalence relations, we looked at, how does one define an equivalence relation, and then we proved some properties.

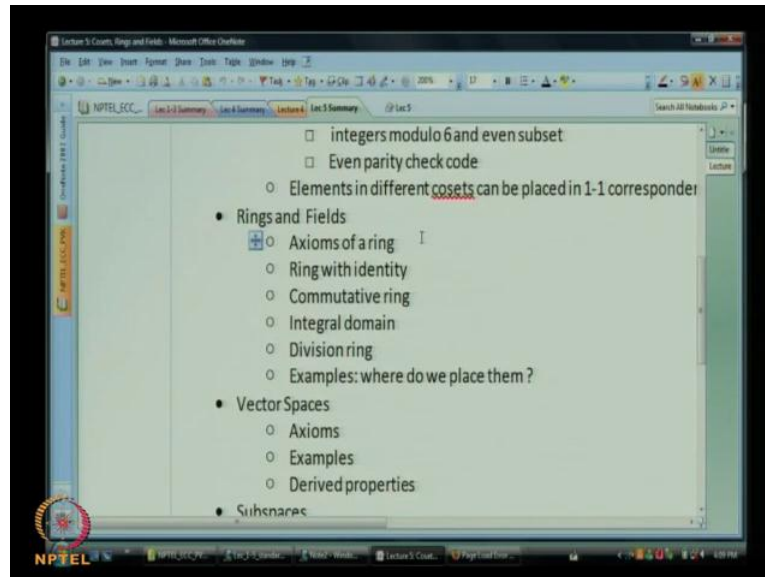
(Refer Slide Time: 03:46)

Lecture Topic: **Cosets, Rings and Fields**

- Equivalence classes defined via cosets:
 - Proof that it is an equivalence relation
 - The nature of the equivalence class $E_b = Hb$
 - Examples:
 - integers modulo 6 and even subset
 - Even parity check code
 - Elements in different cosets can be placed in 1-1 correspondence
- Rings and Fields
 - Axioms of a ring
 - Ring with identity
 - Commutative ring

We talked about the fact that an equivalence relation, so, this is a particular form of relation. It has the property that it partitions the set into equivalence classes; it means that, this set is broken into collection of subsets, which are disjoint. Then we actually gave an example of an equivalence relationship arises from the presence of the subgroup, within the group. We looked at such an example; so that is about where we were. So now, having done this let me also go ahead and tell you, what are planned for the days. So, our plan for the day is to actually talk about cosets, rings and fields. So, we will look at equivalence classes defined via cosets; that is the continuation of what we were doing in the last lecture. Then we will prove, will look at some examples, and we will also give some structure to the nature of equivalence class in this case. We will prove a further property and then after that, so we started out by talking about groups and subgroups.

(Refer Slide Time: 04:30)



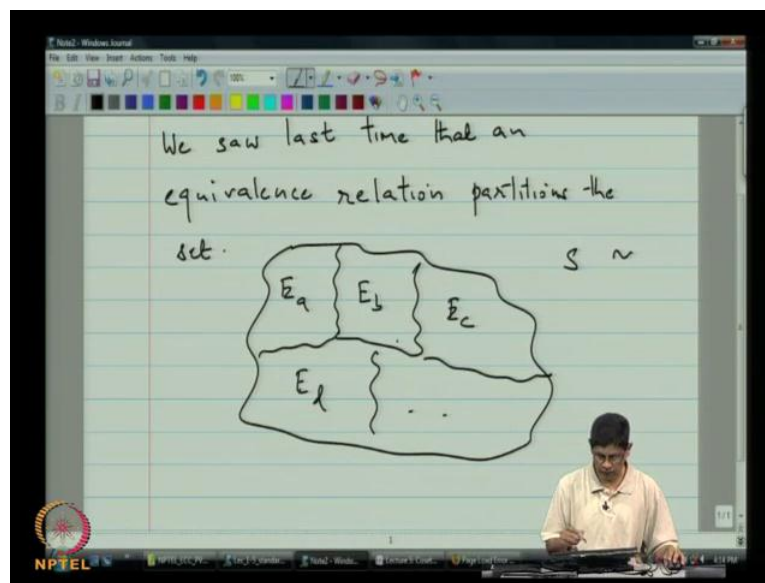
So now, we are going to keep going with our mathematical preliminaries, meaning that we will look at some other algebraic structures, before getting back coding theory. So, we will actually talk about rings and fields; and these are algebraic properties that go, in some sense, beyond those of the properties of group. We look at the axioms that are going to make up a ring. We will talk about the different types of rings, and will end up with fields. Then time permitting will move on talking about the vector spaces. So, vector spaces could take us into the realm of linear algebra, but that is only if time permits.

So, let us go back. Now, I will take you back to the last lecture notes of last time. Let us scroll through that. So, we talked about subgroups and equivalence relationships. We said that, you do not have to test for all the axioms. We looked at some trivial examples of subgroups. That is the group itself, and then the subgroup that consist of a single element, namely the identity element. These are called the trivial subgroups. Testing for a subgroup, you can actually test brute force by checking all the axioms. But, instead of that, there is a simplified test. In which, you just simply check that if a, b are elements in h , when a, b inverses in h .

So, let me prove that this was the equivalent testing all the axioms. This further reduces in the case of a finite subgroups, to just test for closure. Namely, if a and b are in h , that the

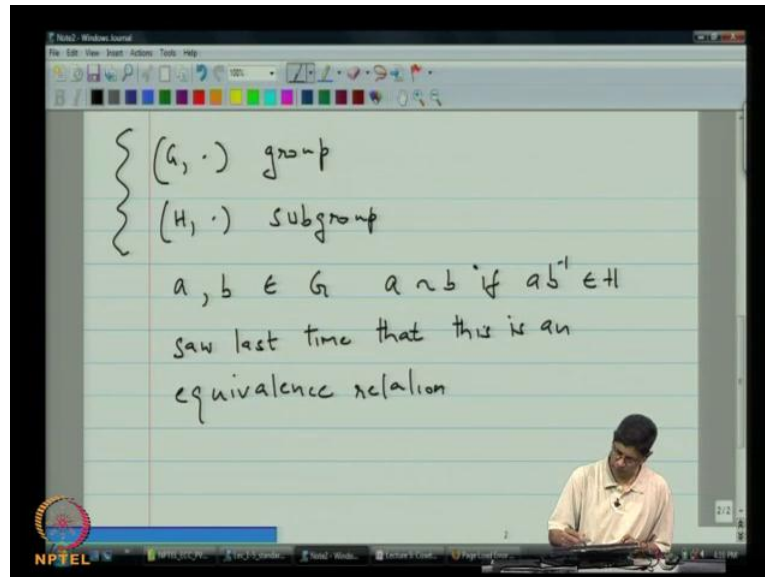
product also is in h . That simplifies to that in this case. Then, we began our journey into equivalent relationships. We defined what it means to be in relation first of all and within the class of relations, we said, we pointed out what an equivalence relation was. It satisfies the properties of being reflexive, symmetry and transitive. Then, the set of all elements that are equivalent to a certain element, let say a , we call that $e \text{ sub } a$. We showed that they have, these have the properties that they either identical for different elements a and b or else they are disjoint. We gave a proof of that and then we talked about the cosets of a subgroup.

(Refer Slide Time: 08:08)

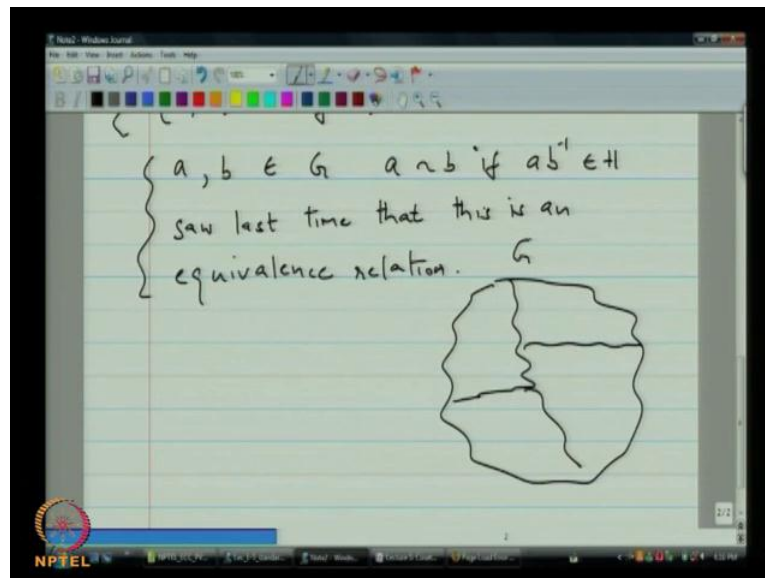


So what, so we are in the setting where there is a group and subgroup and we are defining an equivalence relationship in a manner that involves a subgroup. The equivalence relationship was this, that is, a equivalent to b , if $a b^{-1}$ is in h , alright. We verified there is an equivalence relation and that is about where we were. So, we will continue from that point onwards. So, let me begin now by putting down the title. So, first a quick word about equivalence relations. We saw last time that an equivalence relation, partitions the set. That is, that if you have a set S , and then partitions it into subsets, which are of the form $e a$, $e b$, $e c$, $e d$ and so on. So, that is what we meant when we assign any two equivalent classes or either the same or disjoint.

(Refer Slide Time: 09:20)



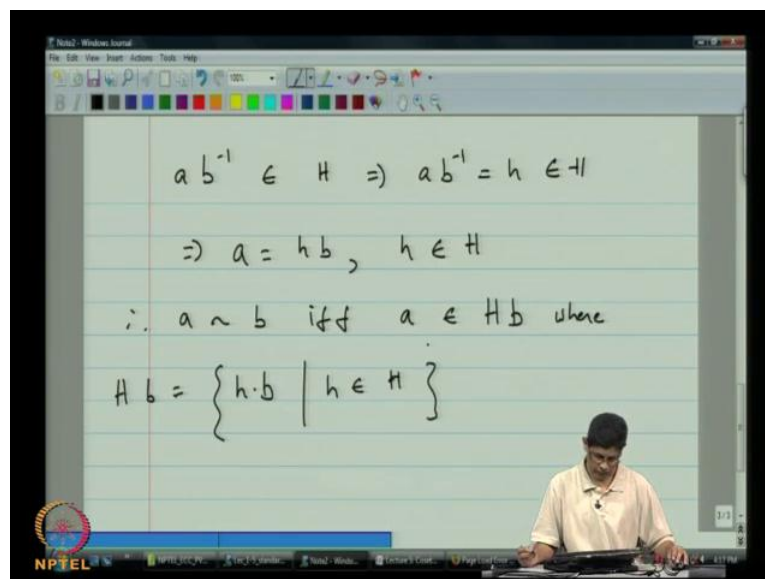
(Refer Slide Time: 10:26)



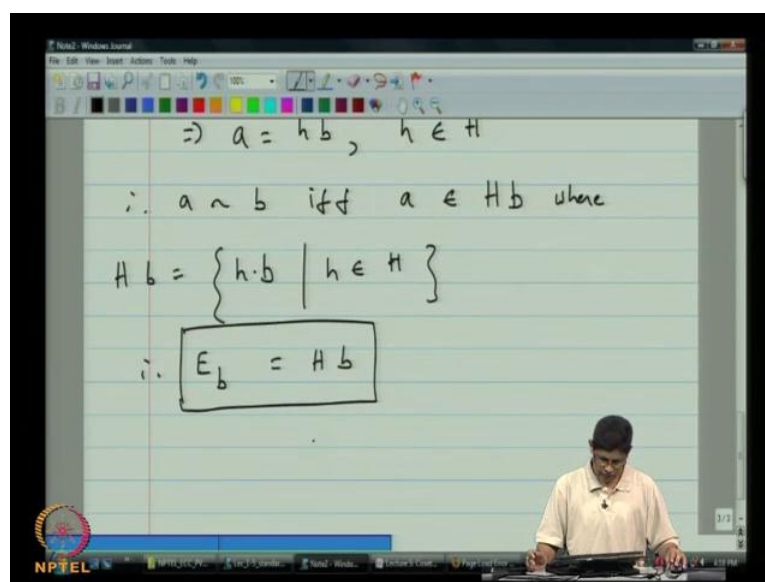
So, if you take the disjoint ones, then they partition the set. Then, we were looking at the equivalence relationship that arises from a subgroup. So, we defined, so, we had a group. So, this was a group. Then, we had a subgroup and we defined an equivalence relationship on the group by saying that $a \sim b$, if a, b are in G , then a is equivalent to b , if $a b^{-1}$ is in H . So, we saw last time that this is an equivalence relationship. So, let us try to get slightly better

field for what the equivalence classes are. We do know from just the fact that there is an equivalence relationship. The following picture holds that you have g and you have some equivalence classes. So, the question is, what exactly are these equivalence classes?

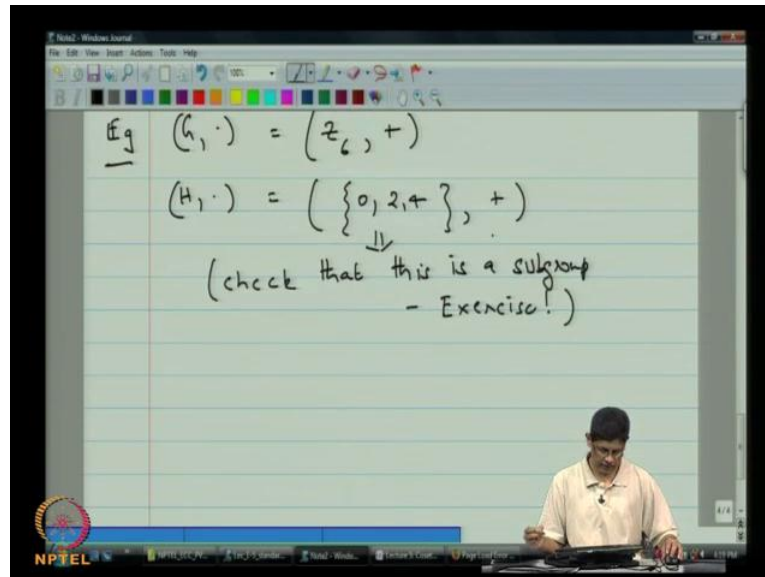
(Refer Slide Time: 10:54)



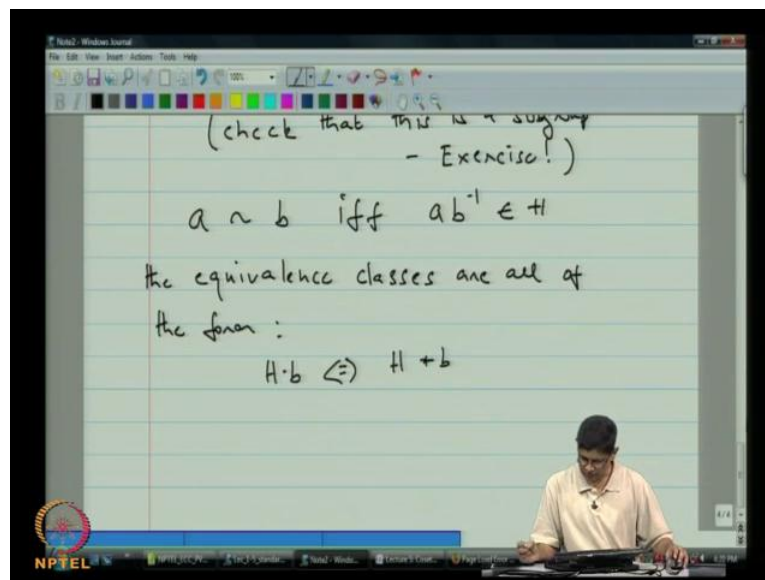
(Refer Slide Time: 12:08)



(Refer Slide Time: 12:32)



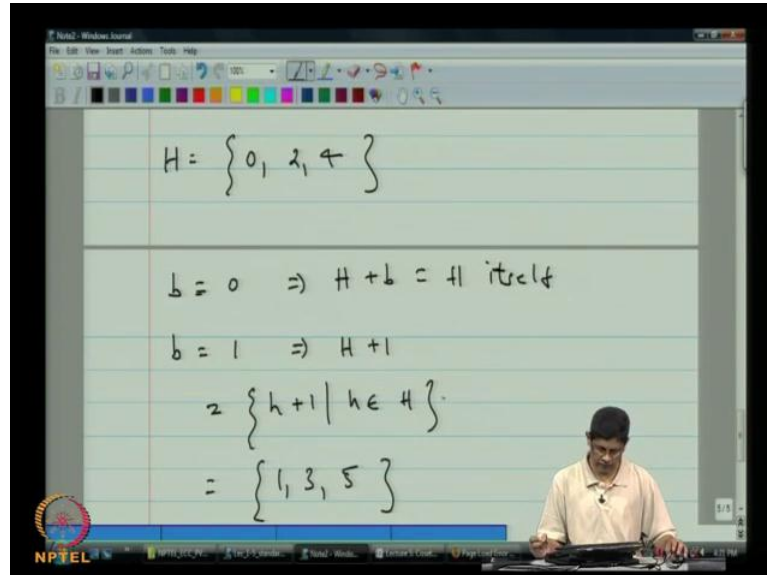
(Refer Slide Time: 13:30)



So, let us, so for that, what we are going to do is we are going to write down this expression $a b^{-1} \in H$ in a slightly different fashion. $a b^{-1} \in H$ implies that, $a b^{-1}$ is equal to h , for some element h in H , which implies that, a is equal to $h b$, excuse me, $h b$ for some h in H . So therefore, a is equivalent to b , if and only if, a belongs to $H b$, where we defined $H b$ to be the set of all elements of the form h times b , where h itself is in H . So, in

other words, therefore, the equivalence class of b , now looks like h times b , in this case. So, just to get a field for this, let us look at some examples. If you take g to be the integers mod six under addition and if you take the subgroup to be $0, 2, 4$, under addition, so you can verify this is a subgroup a . Leave that as an exercise to you.

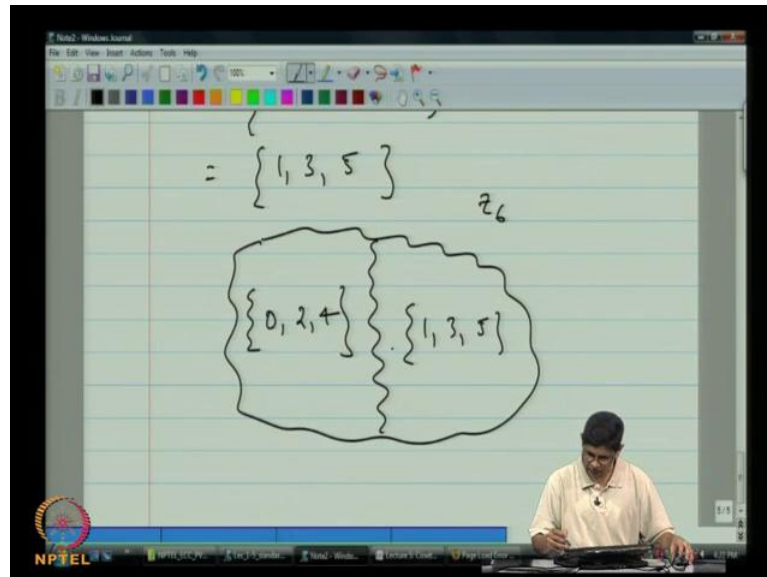
(Refer Slide Time: 14:28)



So now, the question is, what are the equivalence classes, that comes, that arises from saying that a is equivalent to b , if and only if, $a - b$ inverse is an element of h . So, we already seen that the equivalence classes are all of the form $h + b$, which in the present context, since our operation in addition, means h plus b . So, all the equivalence classes are obtained by adding some element to the subgroup. So, since h is the set $0, 2, 4$, you might think of this is even subset of the integers mod six.

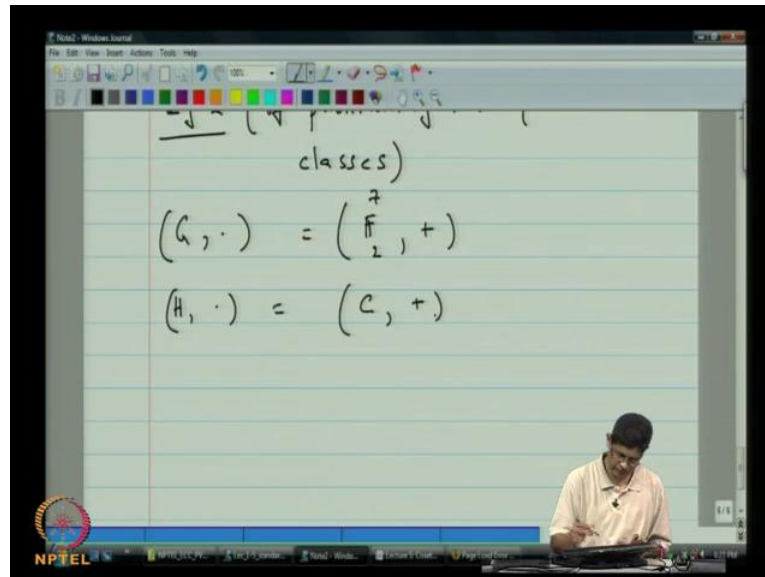
Then, you can actually say that, after all, if you set b equal to 0 , that this implies that $h + b$ equal to h itself. So, one of the equivalence classes is h itself. If you set b equal to 1 , then $h + 1$, remember that this is the set of all elements of the form $h + 1$, where h belongs to h . So, this is the nothing, but, the set $1, 3, 5$. You might think of this as odd subset. We started out with one equivalence class being h itself, which is the even subset and another equivalence classes being the odd subset. But, these two partition it. These two partitions the group.

(Refer Slide Time: 15:34)



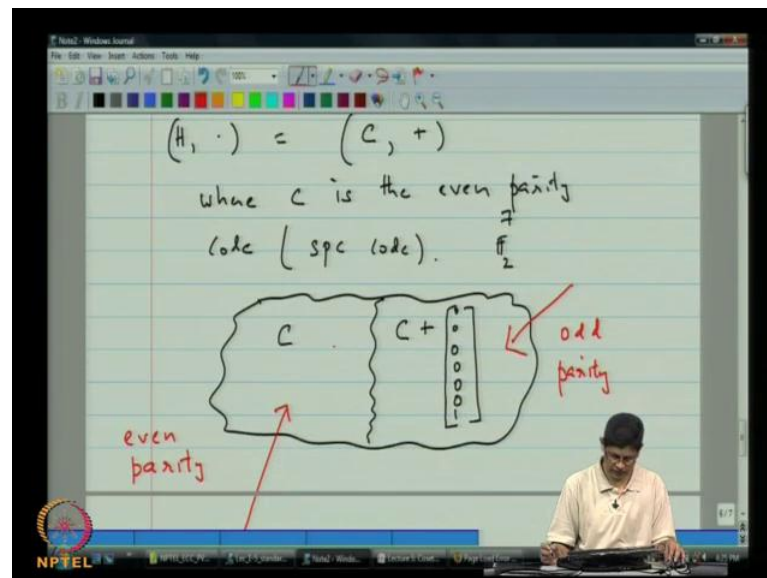
So, we have the following picture, namely, that if we look at the integers mod, this is mod six, and then one side you have the 0 2 4. On the other side, we have 1 3 5. So, these are the only two equivalent classes into which group is partitioned. Why are there no more? Because, if there was a further equivalence class, it must contain some element of z , which means that it either contains one element in 0 to 4 or 1 3 5. But, either way, if it contains 0, then it coincides with equivalent classes of 0. If it contains, let say 3, then it must coincide with the equivalent classes 3.

(Refer Slide Time: 16:48)



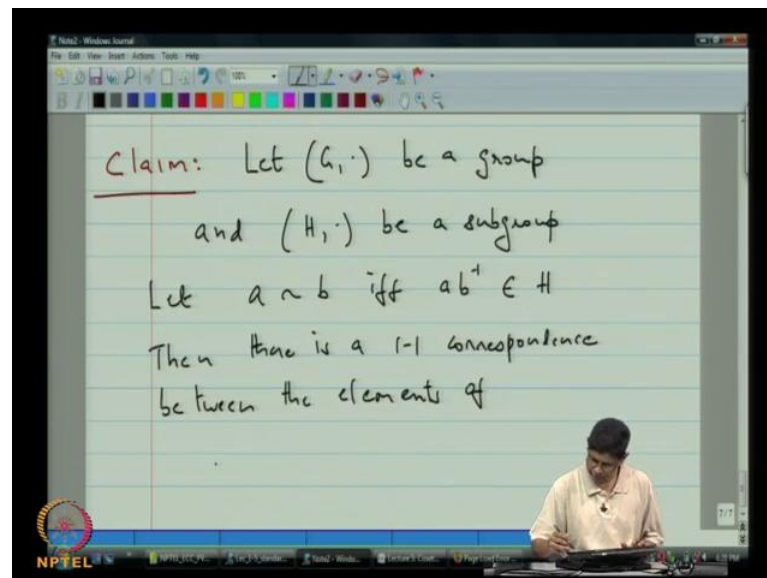
So, these are the only two equivalent classes. That is one example. Now, let us look at second example. So, this is the example of partitioning into equivalence classes. So, this time, let us take g . Let us take g to be the set of all seven tuples and modulo two addition. Let us take h to be code c plus, where c is the even parity code. You also call this a single parity check code. We know that this is the subgroup, because this showed up earlier when we were checking for a subgroup.

(Refer Slide Time: 18:30)

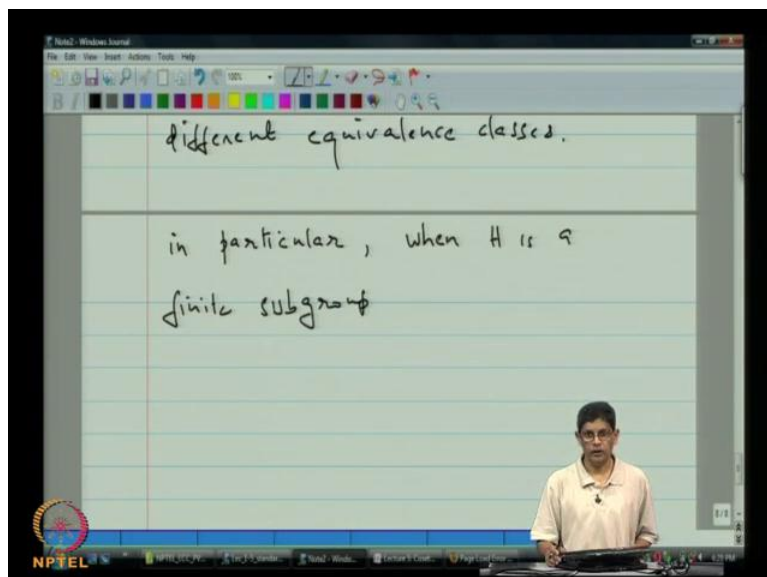


So now, so the cosets, you can verify that in this case, what happens is that the set of all seven tuples, once again is partitioned into two classes; one is the code and the second is the code plus any vector of odd hamming weight. In particular, I can take 0 0 0 0 0 0 1. So, basically what we have here are the even parity vectors; and on this side, we had odd parity. The reason why all the even parity vectors fall into one equivalence class is because simply because that difference also has even parity which means that the difference belongs to h . So, I leave it to you to fill in the details; so will just leave it at that interest of going alone.

(Refer Slide Time: 21:20)



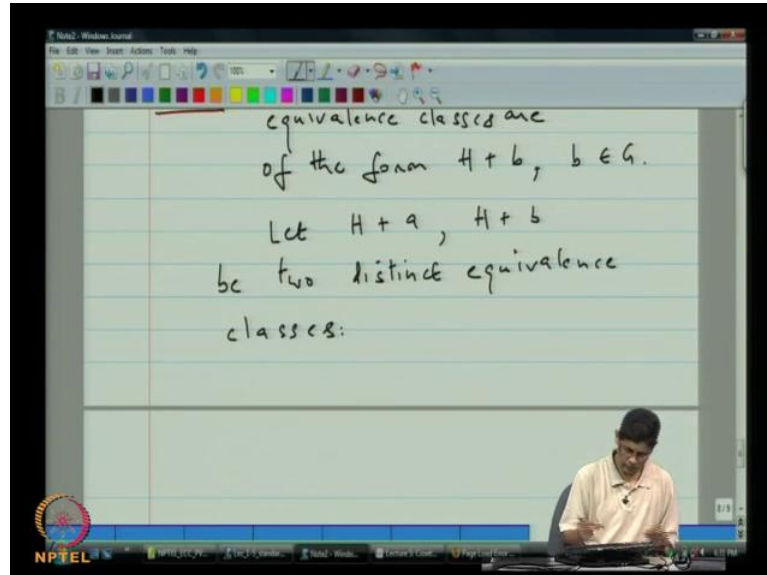
(Refer Slide Time: 22:42)



So, verify that this is the case, right. So, with that we have done with examples. Now, one other property that we will actually use a little later is that when you look at the equivalence classes that arise from the presence of a sub group within a group, that the number of elements in each equivalence class is the same. So, let us go head and show that. So, we will put this down as a claim. Let G be a group, and h be a subgroup. Let a equivalent to b , if and

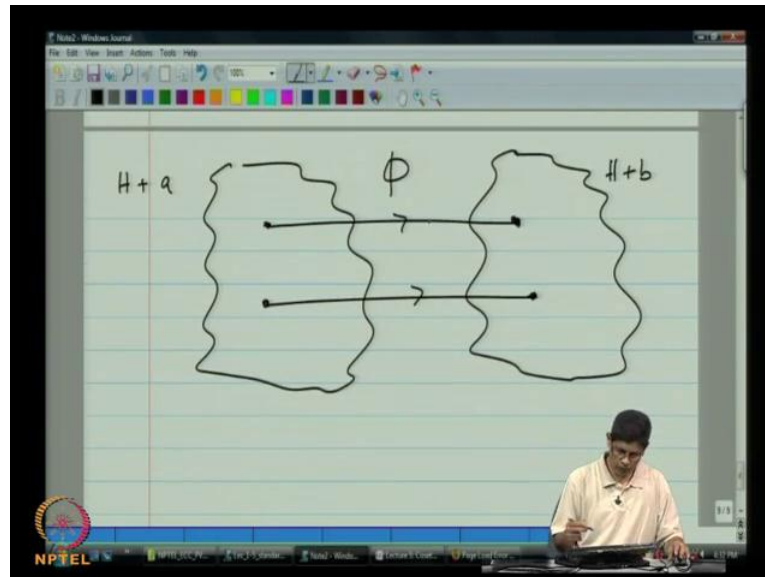
only if a b inverse is in H . Then there is a one to one correspondence between the elements of different equivalent classes. In particular, when h is a finite subgroup; and this will always be the case in coding theory. So, when I say there is a subgroup is a finite, we simply mean that the size of the subgroup is finite.

(Refer Slide Time: 24:16)

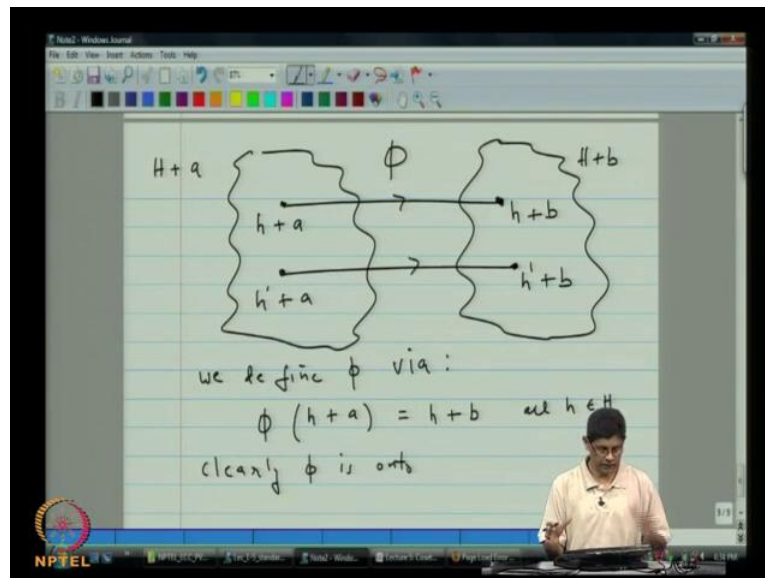


All of our theory of error correcting code will always be dealing with finite subgroups. So in particular, when h is a finite subgroup, any two equivalence classes are of the same size. So, this is our claim. So, the claim is that there is one to one correspondence between the elements of the equivalence classes. Now we know, so the proof. So, the proof of claim, we know that, that all equivalence classes are of the form h plus b , some b in G . So, let h plus a , and h plus b be two distinct equivalence classes.

(Refer Slide Time: 25:30)



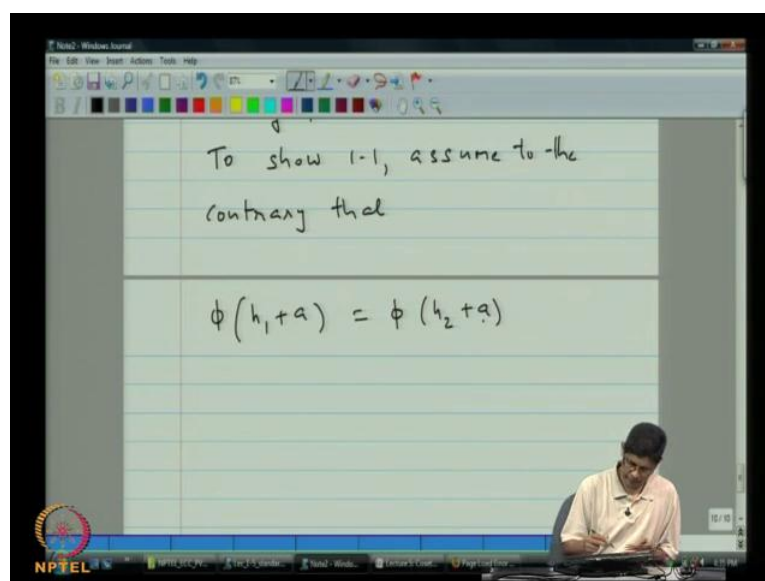
(Refer Slide Time: 26:38)



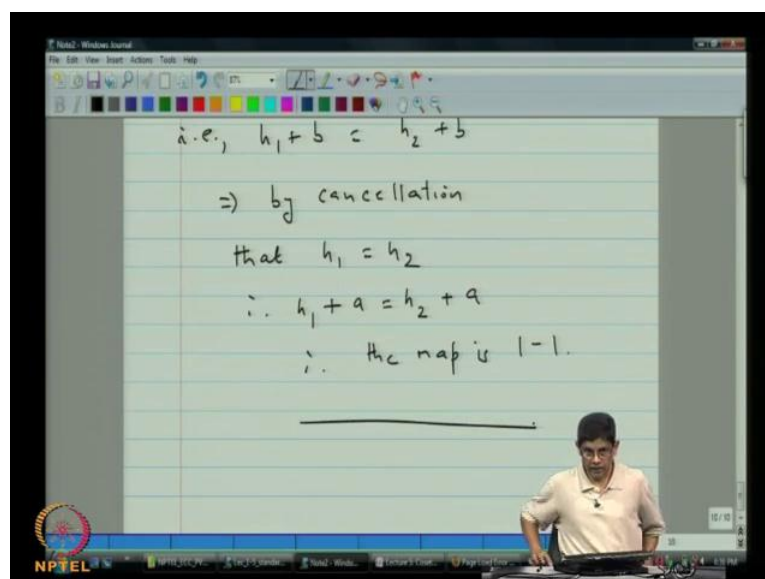
So, we have, so what we want to show is that there is the equivalence relationship, that is the one to one correspondence between the elements of these two equivalence classes. So, if this is h plus a , and if this is h plus b , we want to show that for every element in here, we can actually map to a unique element in here. So, this is a very nice and simple picture in this situation. So, let us call this mapping ϕ . So, this is the mapping ϕ , which is both one to

one and on two. So, the question is, to actually prove this, we just have to show that there is a mapping which is one to one and on two. So, that is mapping fee. We defined phi via phi of a plus h. So, may be to be careful, since it h plus let me be careful and write this as h plus a.

(Refer Slide Time: 28:50)



(Refer Slide Time: 29:24)

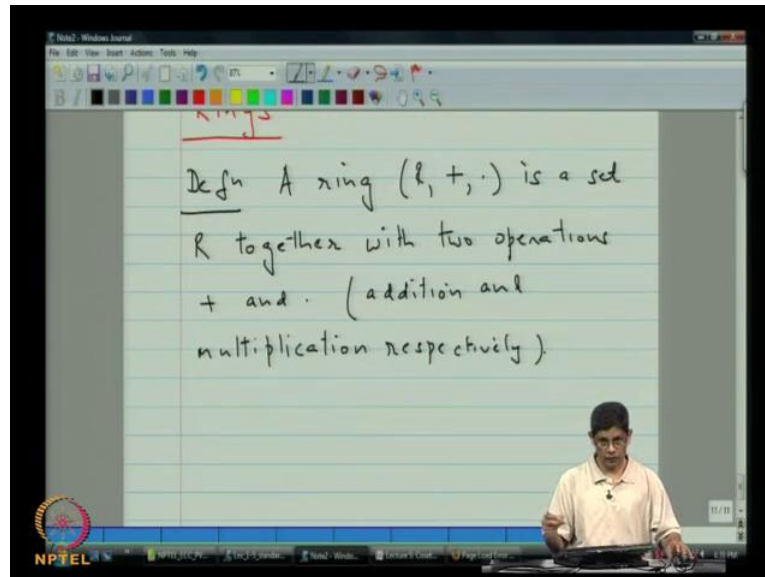


So, this is ϕ of h plus a . If the group was commutative, then h plus a is same as a plus h . But let say we do not know that. Then in the application to coding theory, it will be commutative. So, ϕ of h plus a , will be h plus b for all h in H . Now, clearly ϕ is onto because what is onto? It means, onto means that we just have to show that onto simply means, we have to show that for every element on the right hand side, there is a corresponding element on the left, which ϕ takes and maps onto that element.

But if you go down to the picture here, it is clear that you want to find what, let say that is the particular element here, which is h plus b , let say this is h' plus b . To find out which elements go here, all that you have to do is, you have to take h plus a , and h' plus a . So, there is no problem in showing that the map is actually onto. Now, the question is, how do you show that it is one to one. So, the various, may be ϕ of h plus a and ϕ of h' plus a will map to the same element. To show one to one, assume to the contrary that ϕ of h_1 plus a is equal to ϕ of h_2 plus a , i.e., h_1 plus b is equal to h_2 plus b . But I can simply cancel beyond both sides. It implies that by cancellation, which strictly speaking means that we are going to add b inverse or minus b on both sides. That implies through cancellation that h_1 equal to h_2 . Therefore, h_1 plus a is equal to h_1 plus a is equal to h_2 plus a . Therefore, the map is one to one.

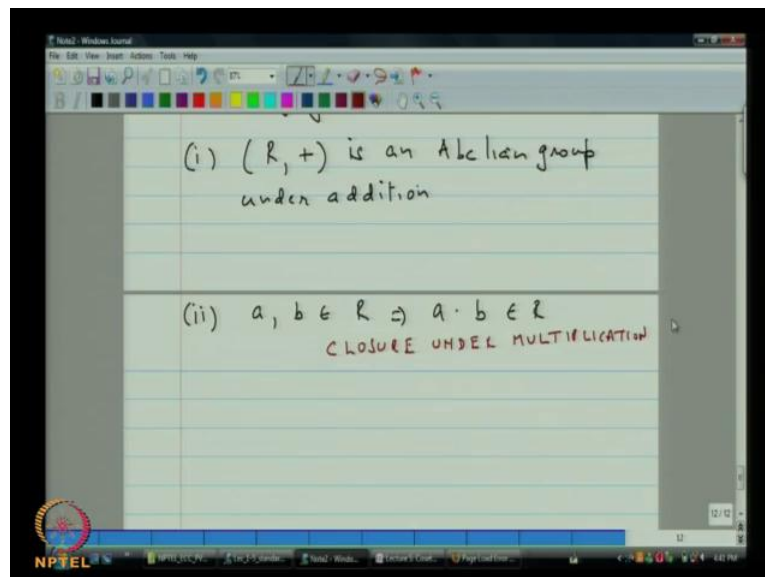
Now, I can understand that there will be a little feeling of impatience as you are watching through this, it seems like a lot of abstract map and you are not sure where you are going. So, apart from asking you to be a little bit patient, I just want to tell you that, we are just building up a simple picture in our minds, which basically is generalization of what you saw in the example of the even parity code. There we saw that the whole set up, all seven tuples was partitioned into equivalence classes and the equivalence classes were in either even parity or odd parity. Of course, the number of even parity vectors is equal to the odd parity vectors. This, similar situation is true in general. It may be that you will have more than two equivalence classes and typically well. But, all equivalence classes are of them the same size and all equivalence classes are going to look like c plus something. So, the code itself will be one of the equivalence classes.

(Refer Slide Time: 32:28)

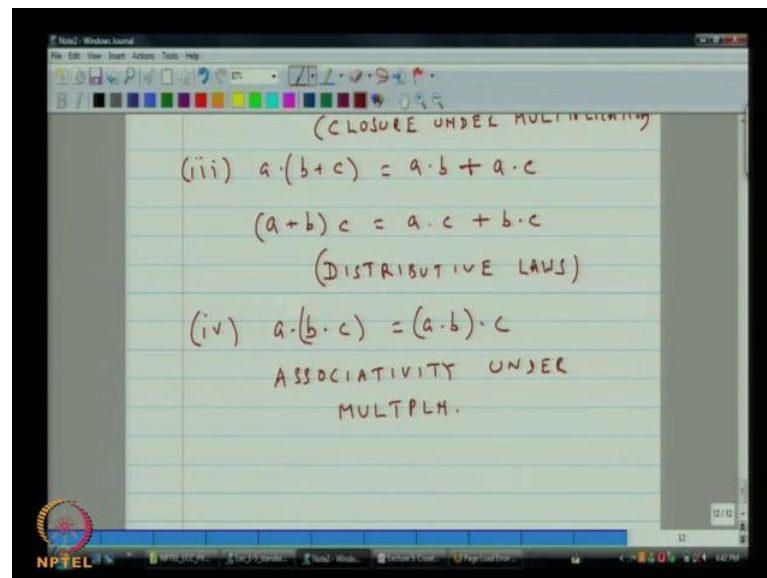


So, this example that we just saw is simple, but, yet the same time failure representative. So, we have done with equivalence classes as of now. So now, would like to move on to talking about a fresh, new type of algebraic structure which is called a ring.

(Refer Slide Time: 34:10)



(Refer Slide Time: 35:14)



So, what is a ring? A ring is a set r together with two operations plus and dot. So, you can think of these as addition and multiplication respectively. So, recall that, when we were talking about groups and on other hand, we just had single operation, right. Just a single operation and then, there were axioms and all were related to that single axiom. Now, for the first time we are actually talking about set. Now, there are two operations. So, that is the difference. So, what we going to do is, we are going to lay down axioms involving both the operations. Satisfying the following, 1 r plus is an abelian group under addition. Secondly, a b in r implies that, a times b is in r . You can say that, this is the operation of closure under multiplication. Then, after that you have the distributive laws. That is, a times b plus c is equal to a times b plus a times c and a plus b times c is a times c plus b times c . These are the distributive laws, right. The fourth property is that, a times and b times c is the same as a times b and c . So, this is associativity under multiplication. So, we have total of four axioms.

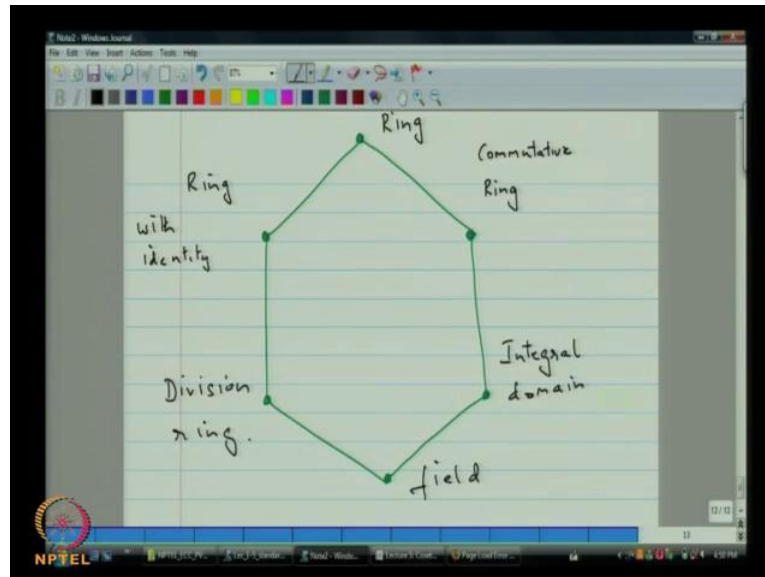
So, the first one actually says, first one confines itself to just single operation. That is, addition. It says there, if you take r and then, if you take addition alone, then r plus must be an abelian group. We know what that means. It should satisfy closure and addition, it must have an identity element, there must be an inverse, and addition is associative. Since it is abelian, addition is also commutative. So, that single first property really can be expanded into five properties. That we have already studied. So, that we have understood pretty well.

So now, we are introducing the second operation, which is multiplication. Then, we are laying down some other rules that it must satisfy. Now, there are three other rules listed below, that is, two three and four. Out of the three, two pertain only to multiplication. So, that two properties pertained only to multiplications are closure under multiplication and associativity under multiplication.

So, these two must be satisfied. Now, if you are thinking in terms of a group, under multiplication, I mean if that was the goal, then in some sense you are satisfying two of the four properties, the other being identity and inverse. But, in reality, we are not going towards groups, at least not yet. So, we have two properties. There is closure and associativity under multiplication. The third property is distributive law. Distributive law is interesting for two reasons. First of all, it is interesting because, it is it is an axiom that relates both addition and multiplication. That is one reason, why it is little bit different from others. But more interestingly and also from an application point of view is that, if you look at just this operation $a \text{ times } b \text{ plus } c$, now think of it as a computation that you are performing.

So, on the right hand side, it is $a \text{ times } b \text{ plus } c$ is $a \text{ times } (b \text{ plus } c)$. Now, if you have to carry out this computation along the lines of what the right hand side suggests, then the total number of operations would be one from multiplying a and b , one from multiplying a and c and third operation to add the two. So, that is the total of three. On the other hand, if you actually look at the left hand side, the left hand side says, it is a smarter way to do it, because I can actually take b and c and add them together and then, multiply by a . So, it is says, instead of doing three, you can actually do two. Now, nobody is impressed. They will say what is the difference? Two or three. It really does not matter. It does not really make a difference. But in practice, yes, that is a big difference, because it turns out that, when you repeated apply distributive law, you can save considerably in the number of operations. In fact, it turns out that this simple distributive law is, in a way, behind the savings in computation, further by simplified decoding algorithms, for very important class of error correcting codes, actually two of them. One is class of low density parity check codes the second is stereo codes. We will come to those somewhere in the middle of this class.

(Refer Slide Time: 40:59)

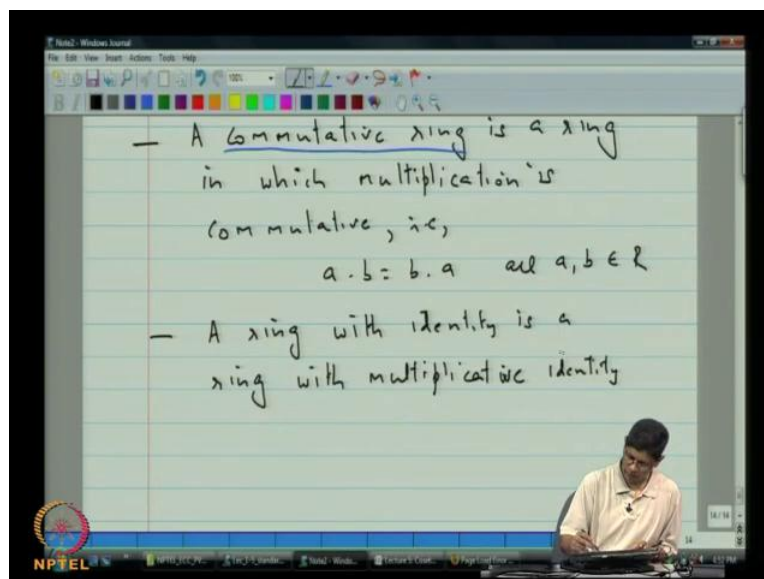


So anyway, so the axioms that make up ring are that, under addition it must be an abelian group and under multiplication, it must be closed and associative. Then it must satisfy the distributive laws. These are the axioms. Now, what I am going to do is, I am going to keep pushing the definitions a little bit further. In interest of keeping you motivated, I give you a preview of where we are headed on this. So, where we headed is the following. We want to organize the various types of rings that exist into a diagram of this form. What are at the corners of these? At the very top, you just have a ring. A ring as we have defined it. Now, to this side, we have a ring, which is commutative. So, we have a commutative ring. On this side, we have rings with identity. Then we have what is called an integral domain. Here we have division rings, and then at the bottom, finally we have fields, a field.

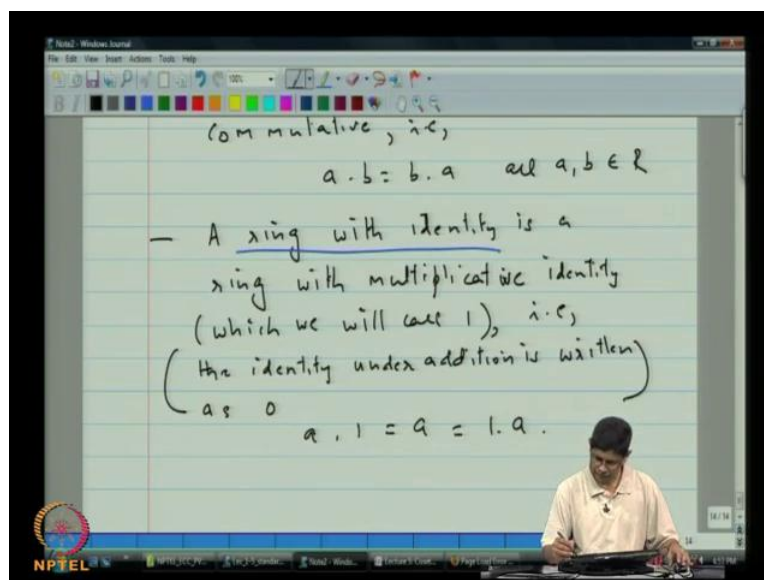
So, in some sense, there is a progression of properties, as you go from top to bottom. There are in some sense, you can progress from being a ring to becoming a field, if you set process certain properties. So, on the way you should interpret this diagram is that start from there right (()), there is a ring; and if under multiplication, if the ring is commutative, then we call it a commutative ring. If further, it satisfies the property of having no zero divisors, so some of these points I will expand in just a few minutes. So, apart from being commutative, if it further, as the property that there are no zero divisors, then it is called an integral domain. Now, going down the other (()), if it is ring with an identity, so that means, you are just

adding the presence of an identity element. Now, **sorry**, as this division ring is concerned, if every non zero element has an inverse, then we say there is a division ring. Then, at the end, we have a field.

(Refer Slide Time: 44:30)



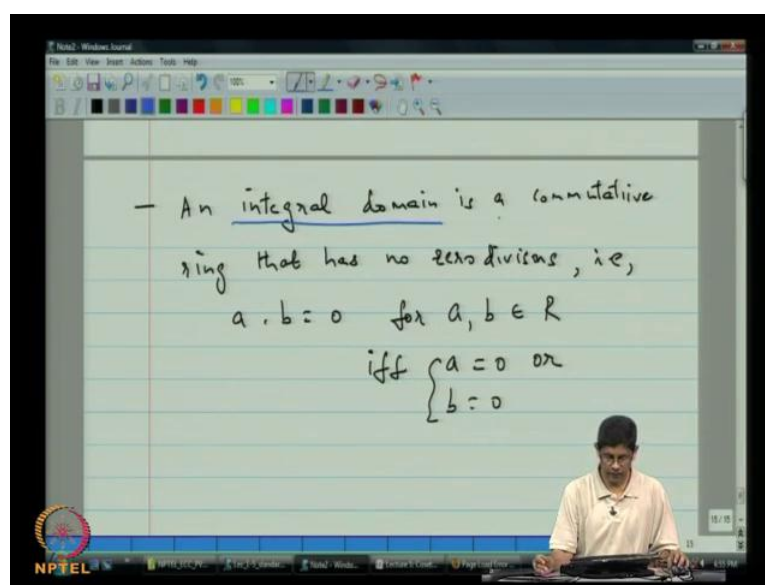
(Refer Slide Time: 46:20)



So, what does a field have? Well, a field has property. It has all of these properties. There is its commutative ring, it is in integral domain, it is a ring with an identity, and it is a division

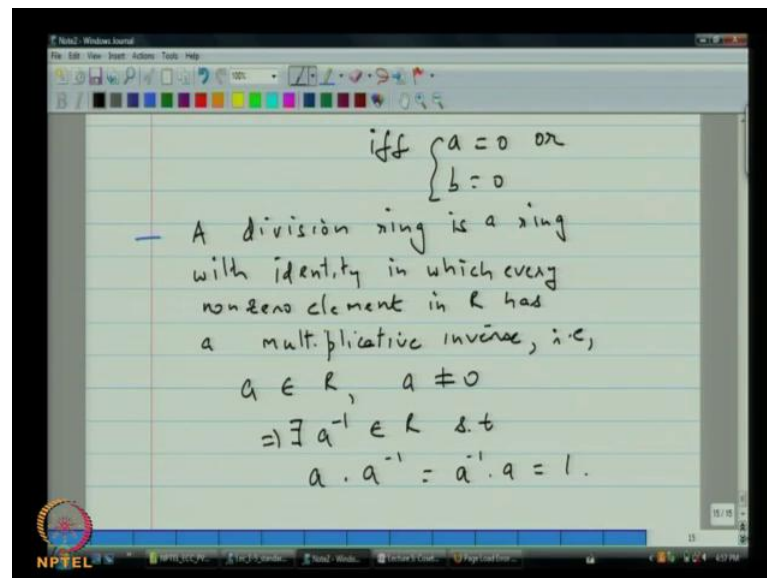
ring. When it has all of these properties, it is called a field. So, I am going to now take out some few minutes to write this out, and then we will look at examples. Some examples of rings, and then we will figure out where to place them on this chart. A commutative ring is a ring, in which multiplication is commutative that is, a times b is equal to b times a , for all a, b in the ring. So, that is the commutative ring. Then a ring with identity is simply what it says. It is a ring with multiplicative identity, which we will call 1. So, here in the context of rings, this identity under addition will be called 0.

(Refer Slide Time: 47:56)



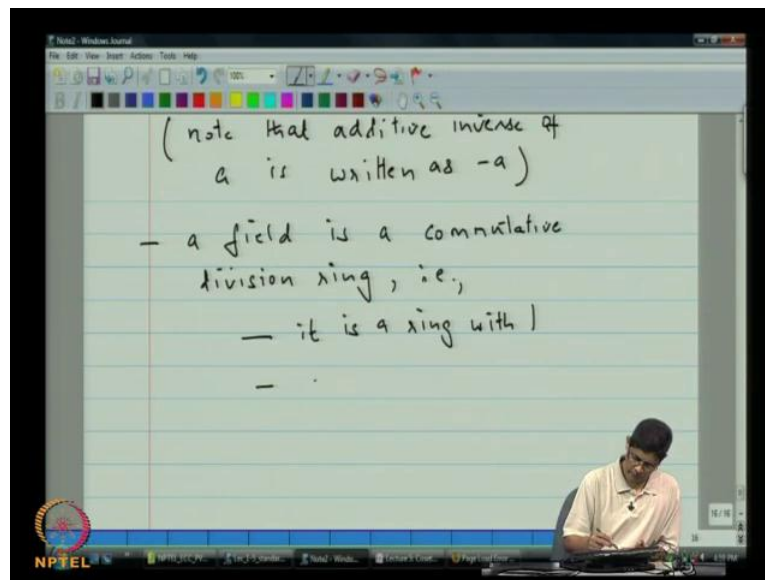
- An integral domain is a commutative ring that has no zero divisors, i.e.,
 $a \cdot b = 0$ for $a, b \in R$
iff $\begin{cases} a = 0 \text{ or} \\ b = 0 \end{cases}$

(Refer Slide Time: 49:26)

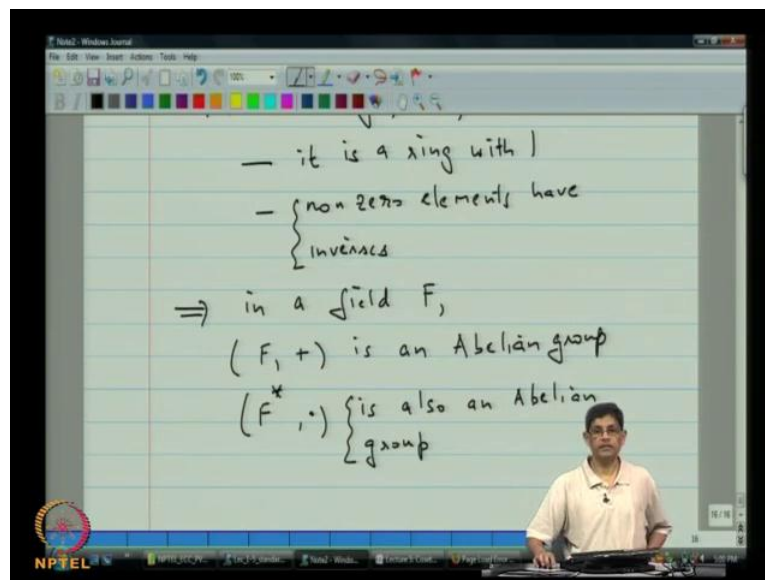


So, the identity under addition is written as 0. So, what this actually means is that, so let say, we will write this as, i e, a times 1 is a is equal to 1 times a . An integral domain is a commutative ring that has no zero divisions, i e, a times b equal to 0 for a, b in R , if and only if, a equal to 0 or b equal to 0. Of course, both can also be equal to 0. But at least one of them must be equal to 0. Notice that, an integral domain requires that the ring can be commutative. So, in a way that is why we listed. In this figure, we listed below. Here the property, it can be commutative and below that, we have integral domain property and finally, we have a field. We have, I am sorry; we have yet another ring, a division ring. A division ring is a ring with identity, in which every non zero element in R has a multiplicative inverse, i e, a is in R and $a \neq 0$. It implies that a inverse, implies that there exist an element a^{-1} in R , such that, a times a^{-1} is a^{-1} times a is equal to 1. Now, by the way, there is also in additive inverse.

(Refer Slide Time: 51:12)



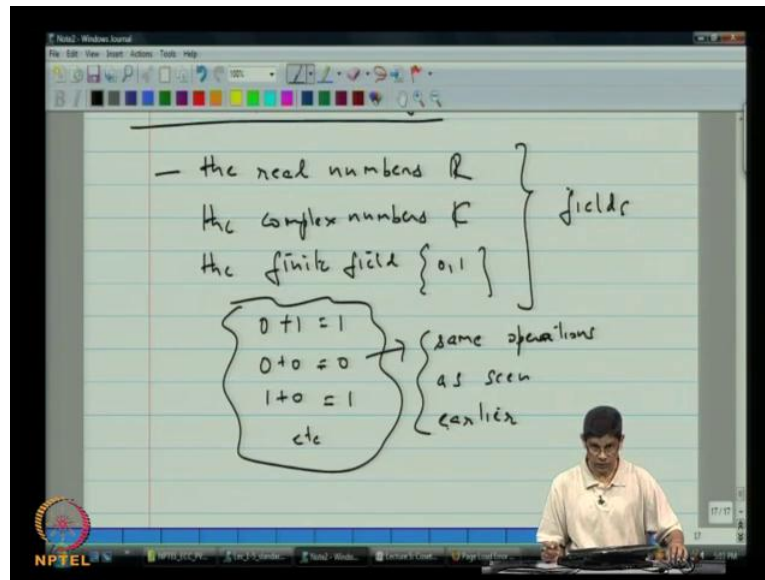
(Refer Slide Time: 52:54)



So, just as a short note, let me just point out that note, that additive inverse of a is written as minus a . So, multiplicative inverse is written as a inverse but the additive inverse is written as minus a . Finally, we have a field. A field is a commutative division ring. Which means that, so let us, which means that the following, it has identity and it is a ring with one non-zero element, have inverses and is commutative. So, as a result of this, we have that in a

field, implies that in a field f , we have property that f plus is an abelian group and f star multiplication and is also an abelian group.

(Refer Slide Time: 55:20)



So, that means, that in a field, so the field is an algebraic object with a lot of structure because, and addition is an abelian group. In some sense, with respect to addition, it has all the properties that we will like and it also has all the properties that we would like with respect to multiplication. But of course, just a note of caution, we cannot define a field just by saying that it is an abelian group and addition and the non zeros and addition form an abelian group, because, there are some axioms, additional axioms. For example, even without excluding zero, the set is closed under multiplication. Also, there are the distributive laws. So, field is more than that. But, it is good to keep in mind that, you have an abelian group, f 2 abelian groups in some sense. One is under addition and other is under multiplication. So now, let us go ahead and look at some examples and we will figure out where it put them. So here, so examples of rings; so first of all, let us look at the real numbers.

So, this is r or the complex numbers. See, r , the finite field $0\ 1$. You can readily check that all these are examples of fields. Now, what I have called here is $0\ 1$. I may not have referred to as a field earlier, but, this is the same set, under the same set of operations that we carried

out earlier and namely that $0 + 1 = 1$, $0 + 0 = 0$, $1 + 0 = 1$ etcetera. So, under these same operations as seen earlier, these are all the examples of field. So, in the figure, we can actually go ahead and put these down here. So, \mathbb{R} , the complex numbers, and \mathbb{F}_2 , all of these are examples of fields. Now, what we will actually do in the next class is, we put down some other examples. I will close with one other example for today.

(Refer Slide Time: 40:59)

The set of integers so since we are close to finishing time perhaps, I want to write it out but I will just say it in words with respect to this figure. The set of integers forms an integral domain and that is reason for the definition. But since our time is up, just to summarize, we looked at equivalence classes arising from a subgroup and we saw they partition the group. We looked at examples, then we talked about different type of rings and we finished defining them, and we were going to look at some examples. So, we will continue from this point onwards, right. So, thank you.