Error Correcting Codes

Prof. Dr. P. Vijay Kumar

Department of Electrical Communication Engineering

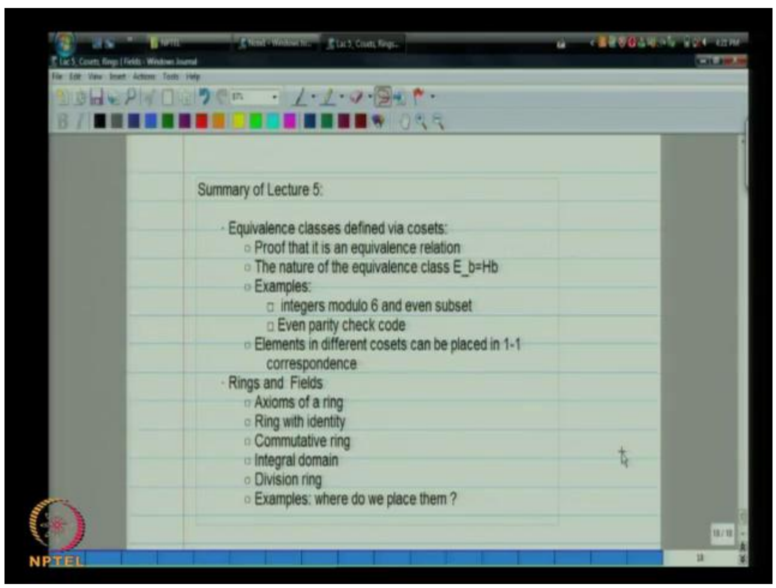
Indian Institute of Science, Bangalore

Lecture No. # 06

Vector Spaces, Linear Independence & Basis

Welcome back to our lecture series here. So, we will begin with I believe our sixth lecture and as we are going along, I am also learning to work with this software and with the tablet pc here.

(Refer Slide Time: 00:39)

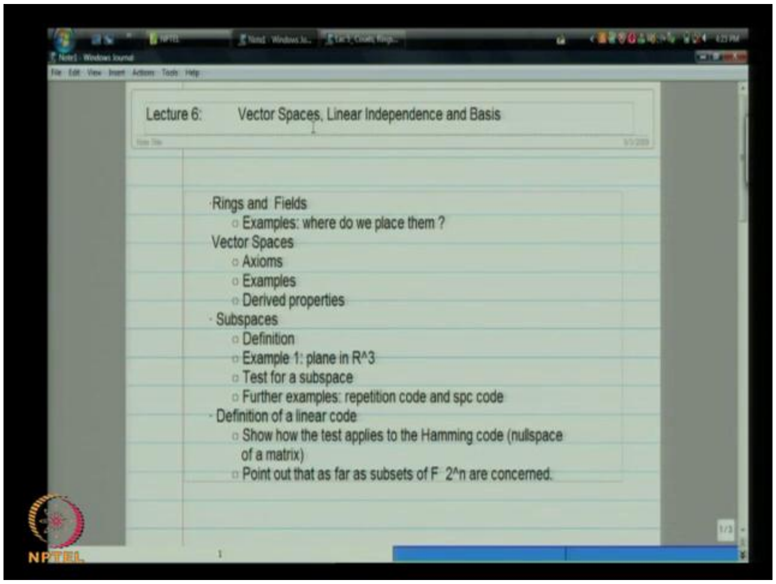


So, let me begin this way today, I have summary of the lecture on the pad and maybe I will just zoom in a little bit to make it a little bit more clearer perhaps, and then we will scroll down to see, I think that should be very visible. So, this is summary of what we did in the last lecture. We first started out by defining equivalence classes, defined by starting from a group. One thing I realized after finishing the last lecture was I did not actually mention the word coset. So, the equivalence classes that we defined which originated from our sub group are actually called cosets. So, I will correct that and I will begin my lecture today by giving a formal definition of a coset.

So, those equivalence classes that arose from groups, we will looking at that and we looked at the structure of an equivalence class that arises in that manner. We looked at some examples, then we showed that elements in different equivalence classes can be placed in 1 to 1 correspondence.

After that with that we were done with the groups and sub groups and equivalence relations. And then we moved on to talking about another algebraic structure, namely we are talking about rings. And we laid out what the axioms of a ring where, we looked at ring with identity, commutative ring, integral domain, division ring. So, we will pick up the discussion from where we left off in the last lecture. And we look at some examples. So, we will do that today and also I think it might be instructive to also show you what are plan for today's lecture is...

(Refer Slide Time: 02:40)

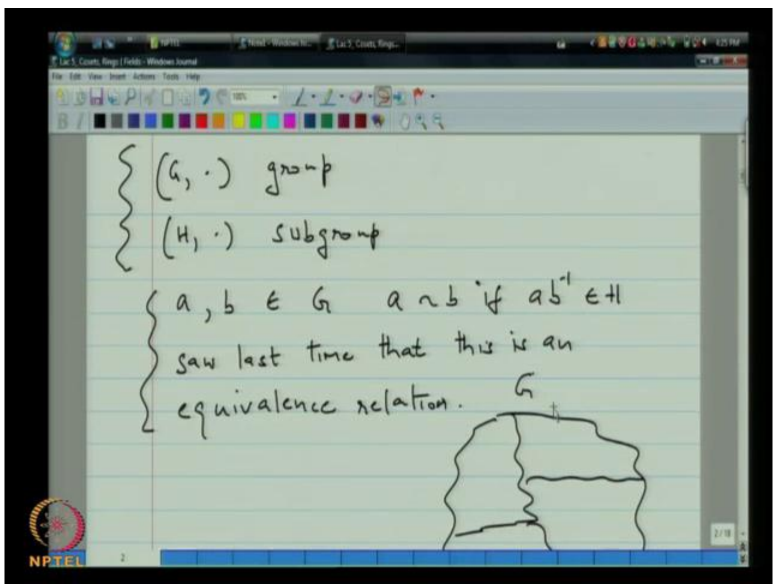


So, today the first topic that we will consider is to finish up the discussion on rings and fields by actually providing some examples. After that will move on talking about vector spaces, so this is taking as into realm of linear algebra. Again now of course, some of you all may have had the requisite linear algebra. But I am going to assume that you do not, and then so in some sense this is an attempt to make the course self contained.

So, we will talk about vector spaces, we will talk about the axioms by which they are defined. We look at examples, derived properties, subspaces, examples, test for subspaces, further examples. Then we will talk about, then we will get back at that point we will be ready to resume our discussion on linear codes and we will begin talking about the class of linear codes.

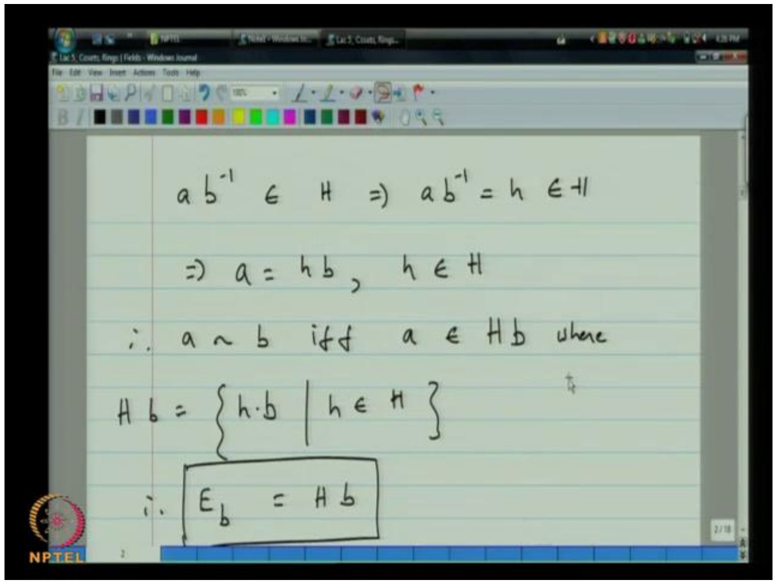
So, that is roughly our plan for the day. Now, so the first thing that I want to do today is talk about coset. So, here we have a page. So, this is like trying to take care of something that we did not completely finish last time. So, let me take the discussion back to the equivalence classes that arose from a subgroup.

(Refer Slide Time: 04:19)



So, in this in this example that we looked at last time, the relation arises in this way you have a group, you have a sub group, and a and b are declared to be equivalent, if a times b inverse belongs to the subgroup and we saw that this is an equivalence relation.

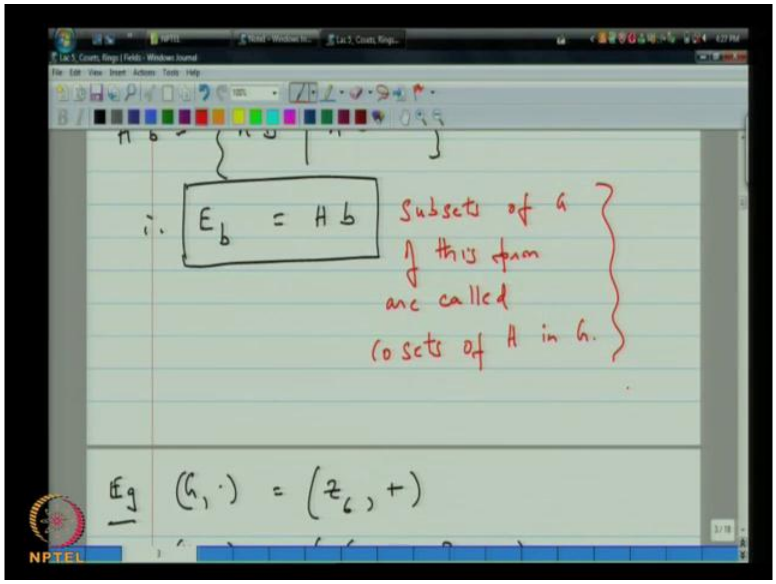
(Refer Slide Time: 04:41)



Now, we want to then we moved on to give different description, of these sets E sub b. Remember we defined certain subsets, and we called them E sub b. This is the set of all elements that are equivalent to b. But in the case of this particular relation they happen to be of the form H times b H times b needs a definition because you have a set multiplying an element.

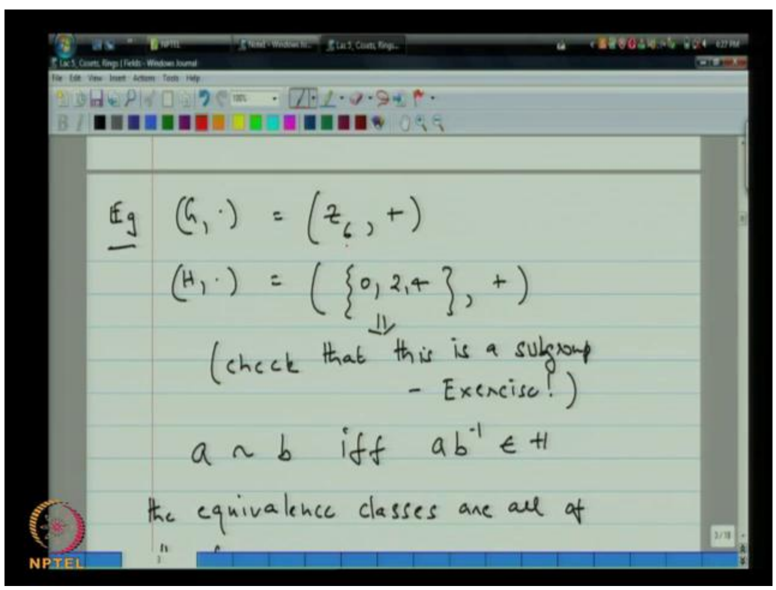
So, that is just simply defined as all products in which b multiplies on the right side all the elements in H. So, these were the things and we looked at examples. Now, it is precisely these elements that are actually called cosets. So, I think it is appropriate to put this to make a note right here, and I will do it in red so that it stands out on the notes.

(Refer Slide Time: 05:50)



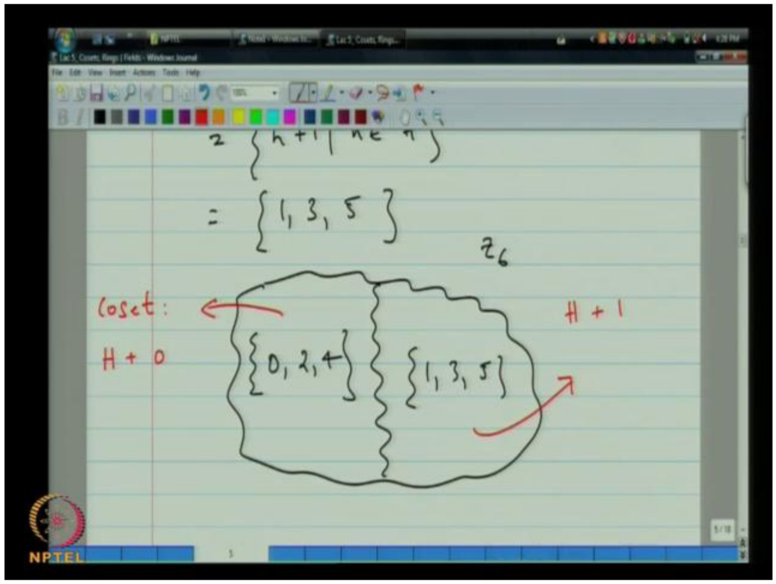
So subsets of G of this form are called cosets of H in G. So, this set is an example of a coset.

(Refer Slide Time: 06:25)



Then the group is the integer mod 6 and H is the even subset of Z 6.

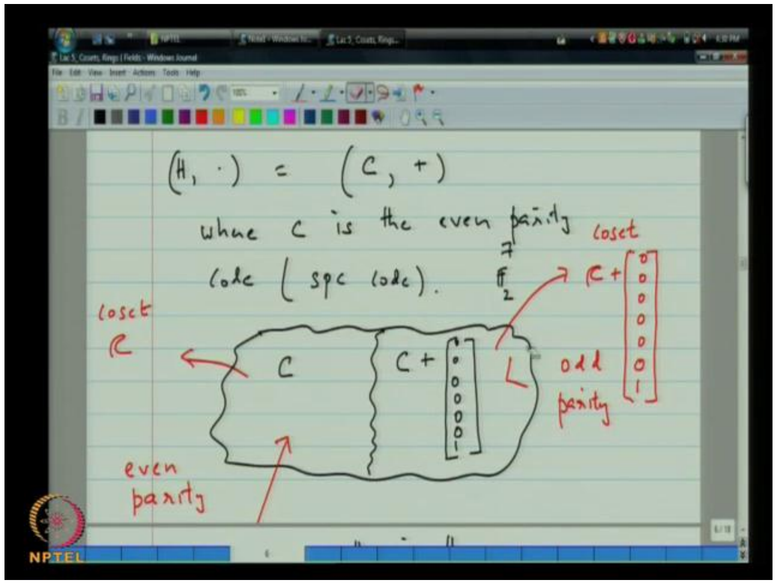
(Refer Slide Time: 06:42)



Then we saw that the cosets of the subgroup there are only 2 of them, one coset is 0 2 4 and the other is 1 3 5; so again trying to make to bring in the notation the terminology of coset. So, this subset here corresponds to the coset H plus 0 and this subset here corresponds to H plus 1.

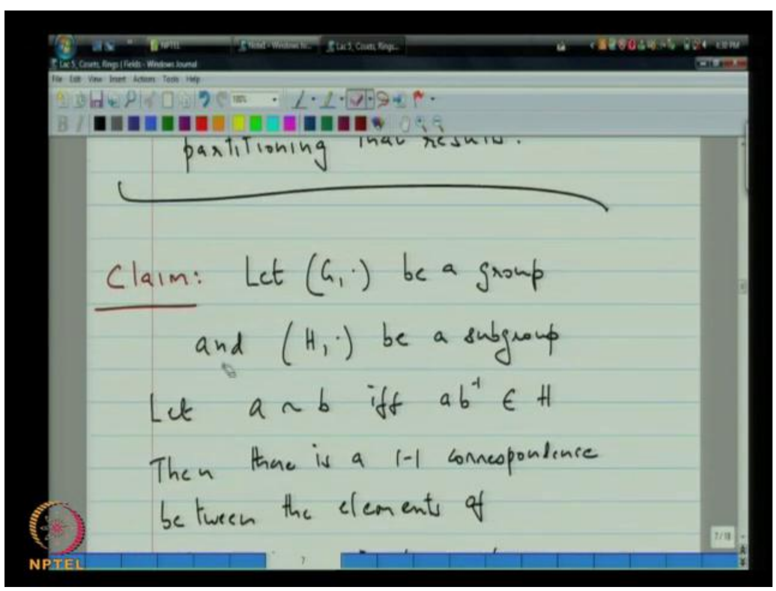
Now, you might ask I thought you defined it as H b well that is because our operation here is addition. So, H times b gets replaced by H plus b and in this case it turns out that there only 2 cosets H plus 0 and H plus 1.

(Refer Slide Time: 07:33)



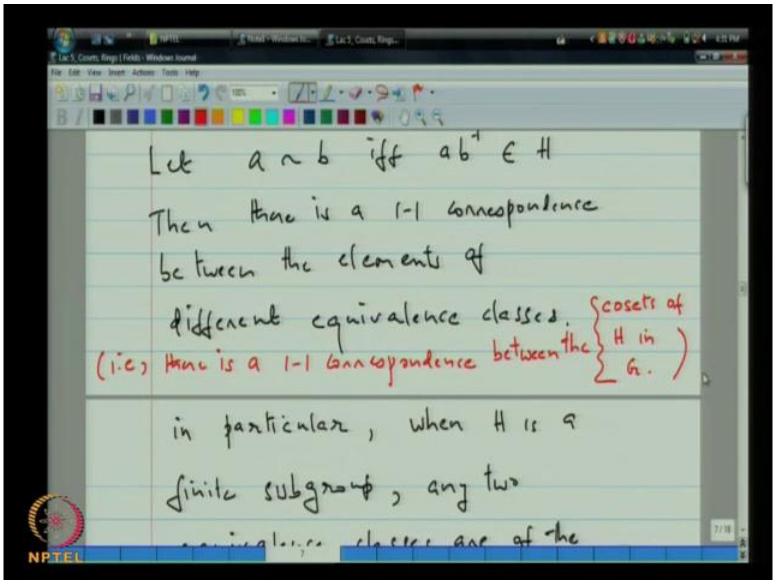
Then, we also looked at another example in which the group itself corresponds to the set of all binary 7 tuples. The sub group is the even parity or the single parity check code and then it turns out that the equivalence classes of cosets are just C and C plus 0. So, again this is the coset this is the coset C and this is the coset this is the coset C plus this particular vector. And I think perhaps we have too many arrows, so let me just erase this.

(Refer Slide Time: 09:09)



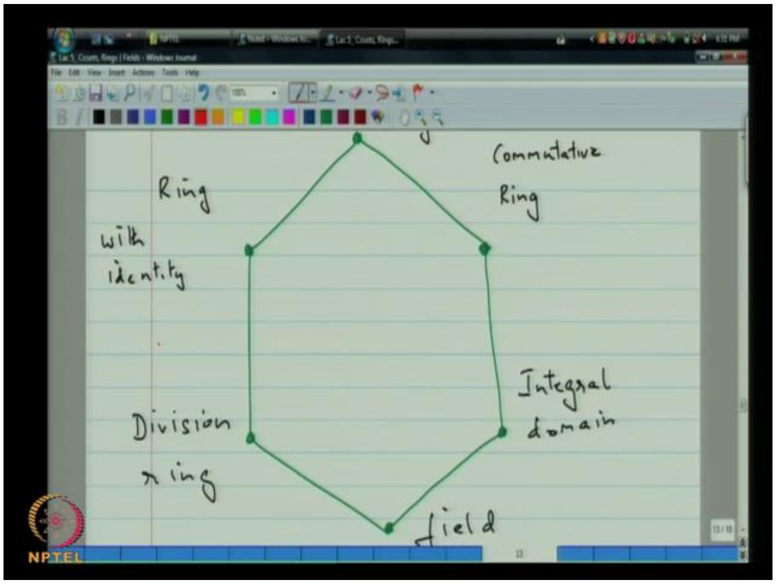
And also further on we actually showed that the equivalence classes is the 1 to 1 correspondence between elements of different equivalence classes.

(Refer Slide Time: 09:17)



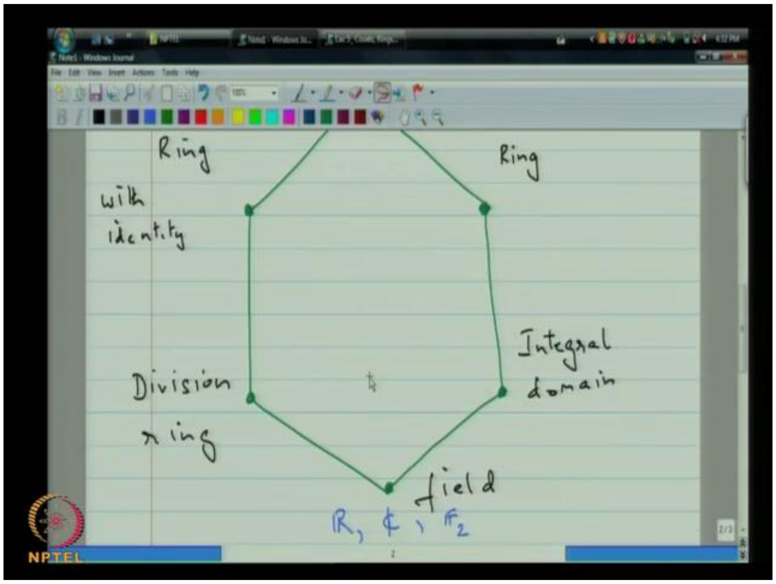
So, you can also rephrase that and say that there is i e, there is a 1 to 1 correspondence between the cosets the the cosets of H in G. So, I think with that I have remedied my over sight in not introducing the coset terminology like last time.

(Refer Slide Time: 10:20)



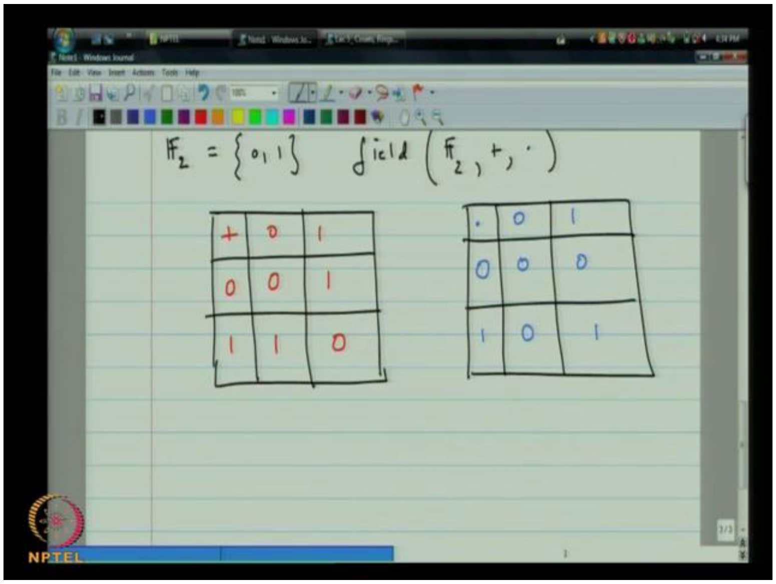
So, with that we will continue on the topic of rings, so where we left off last time was we had defied these various kinds of rings. There was the ring the ring with the identity, the commutative ring, the division ring, integral domain and a field. Now let us move over to our current lecture. (Refer Slide Time: 02:40) So, our current lecture we began with this over view.

(Refer Slide Time: 10:34)



And I have reproduced here for the sake of convenience this ring diagram, that we had last time. In terms of examples, we put down certain examples R C and F 2 and I also thought it is good to say a few words about F 2.

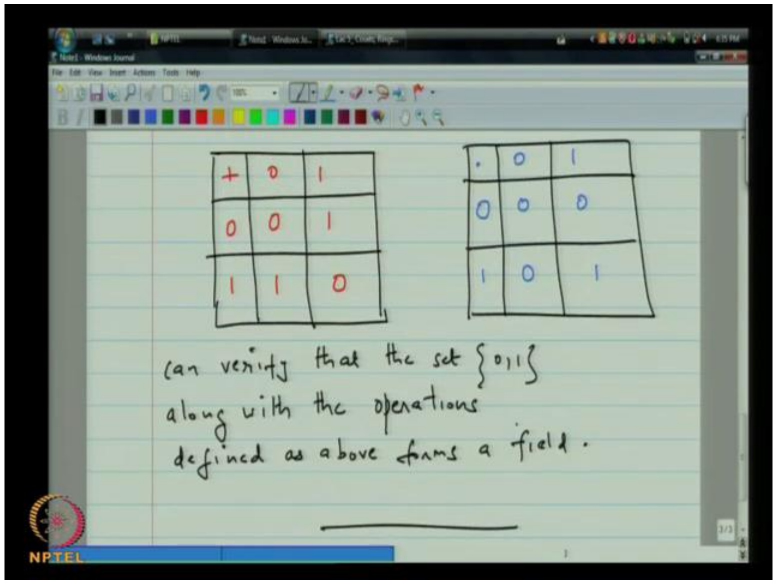
(Refer Slide Time: 11:00)



Now, here F 2 is just the set 0 1 or that is one way of looking at it. But you could also look at it as a field. It is also a field, if you think of it as F 2 plus and multiplication and we had written down sometime back tables governing how addition and multiplication take place and again I thought that, just for the sake of clarity I am going to actually reproduce that here. It will not take more than a minute.

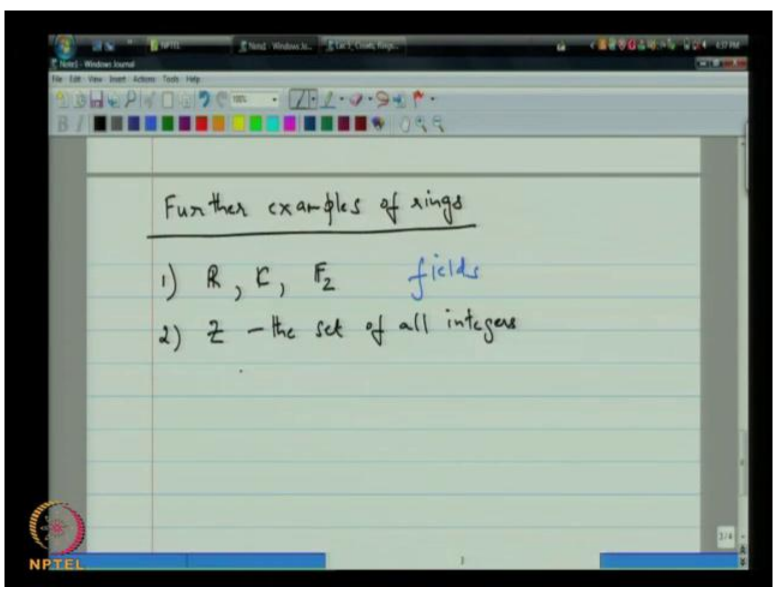
So, this is under let us say plus so you have 0 1 0 1, this is dot and you have 0 1 0 1. So this when you add you get is 0, you get a 1 a 1and a 0. So this is because you are doing modulo 2 addition and here there are no surprises. This is 0 0 0 and 1. Now, it turns out that this set along with these 2 operations satisfies all the conditions to actually make it a field and further being a field it has only 2 elements, so it is called a finite field. In fact, it turns out that amongst the class of finite fields. This is the smallest possible finite field.

(Refer Slide Time: 13:12)



So, let me just make a note of that. Can verify that the set 0 1 along with the operations above defined as above forms a field. So again that was a clarification. So that means that, we are now clear why it is that we have these three examples sitting here. So, on the topic of rings I would like to introduce some other examples as well.

(Refer Slide Time: 14:26)



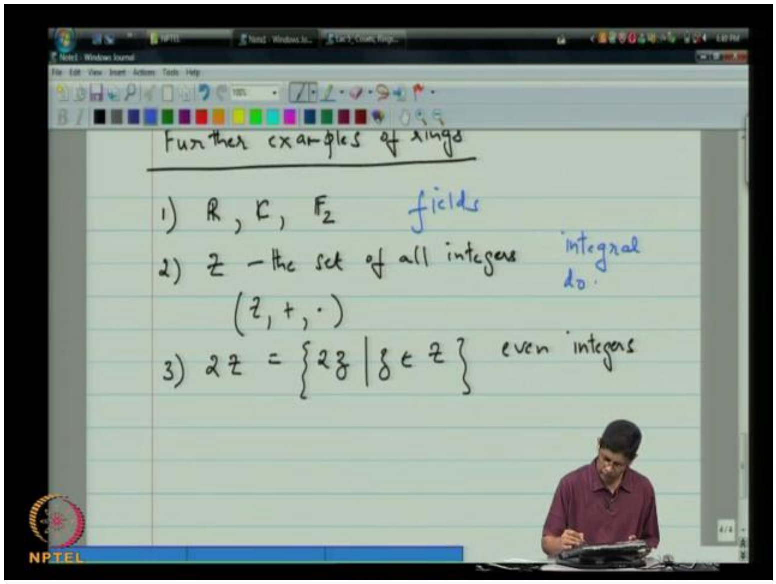
So further examples of rings. Let us take 1: the set. So, I mean in terms of listing we have already seen R C and F 2. So, these are all fields so in terms of saying what kinds of rings are these? We have already seen that these three are examples of fields. Then you can also look at Z: the set of all integers. So that means that you are including positive, negative and the element 0. So what kind of a ring is it? So let us go back and look at this figure here. (Refer Slide Time: 10:20)

So, certainly you can check that it is a ring. So, here I guess I should point out that of course, when you talk about a ring, strictly speaking one should specify the operations. But these are just the usual addition and multiplication and it is not hard to see that the axioms of a ring are satisfied. And further you can also certainly we know that multiplication is commutative so we have no problem there.

And in fact it is also an integral domain because if you multiply the only way you can get 0, by multiplying 2 integers is if one of them is 0, and that condition is the defining condition for something to be an integral domain, and in fact the name in terminology integral domain arises, because the integers are the simplest possible examples.

So in terms of where do we put Z the most appropriate place put it is here. Now, you can also ask well why is in to field? Well for example, elements in the integers do not have inverses. So, you cannot actually call it a field. Could you also put Z over here? You could also put Z here if you liked, because the integers do have the identity, namely the multiplicative identity which is 1. So, it is an integral domain, it is the ring with the identity, but is neither a division ring nor a field.

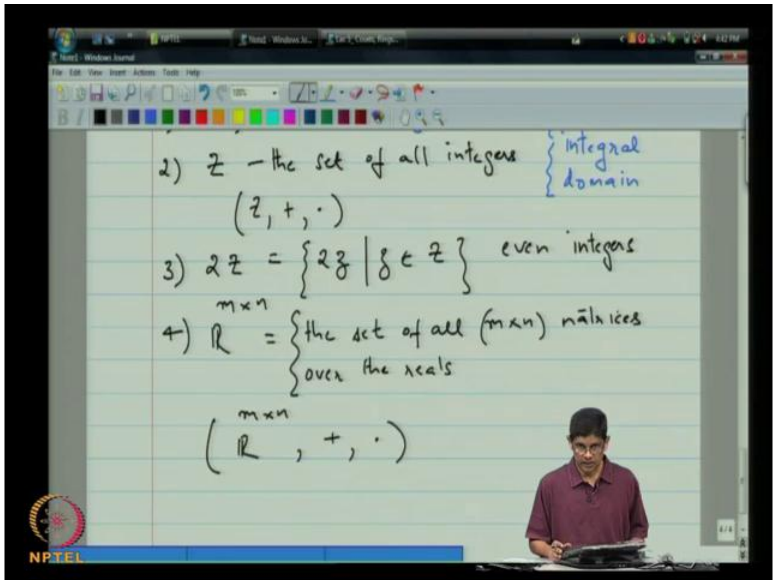
(Refer Slide Time: 17:36)



Three: now, let us make a slight variation an actually defined 2 Z .So what is 2 Z? 2 Z is nothing but the set of all elements 2 times z, where z belongs to Z. So in other words this is all even integers. By the way, we already decided that this was an Integral domain. It is also Ring with identity, but I will not mention that here. Then 2 z is the set of all even integers.

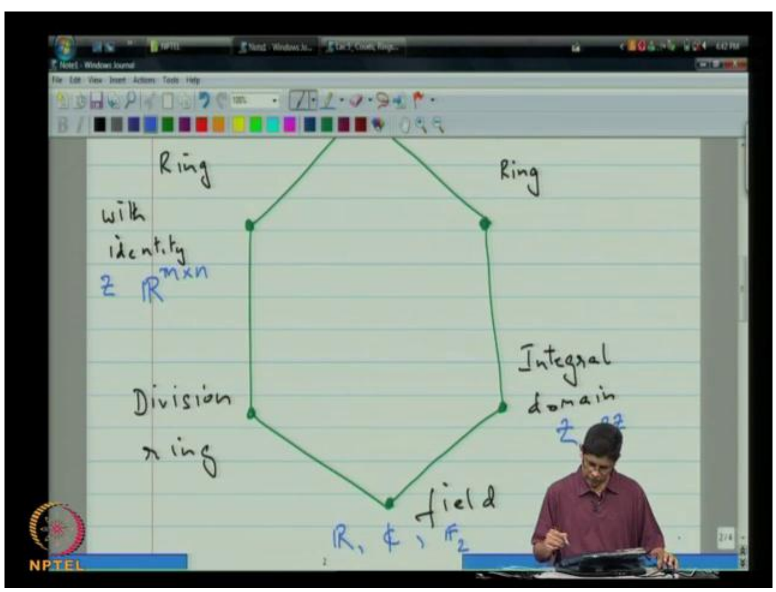
So, let us now go back I think I have a way of going back, here we go. (Refer Slide Time: 10:20) So if you look here then certainly it is a ring and even the even integers if they are commutative. But in terms of then if you ask the question are they an integral domain? Yes they are an integral domain. But are they a ring with identity? So, the different between Z and 2 Z is that 2 Z can be listed here. But 2 Z cannot be listed as a ring with the identity. Now, let us then move on to different type of example.

(Refer Slide Time: 19:22)



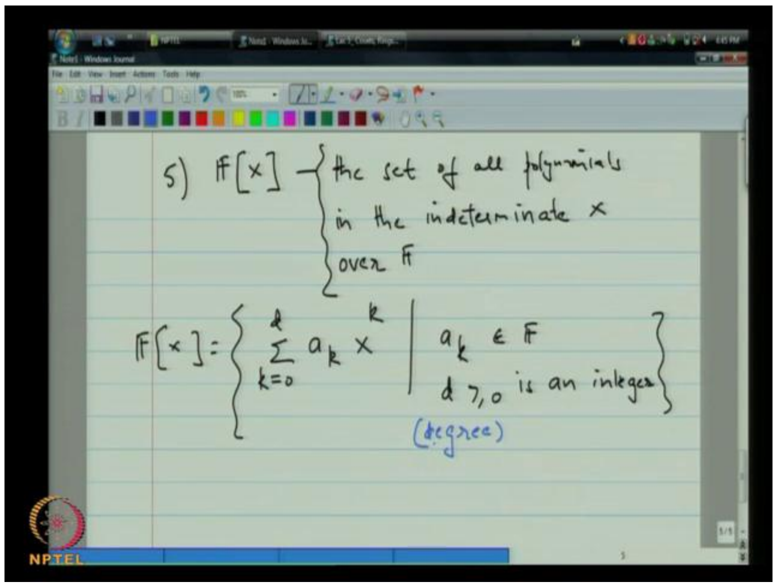
Supposing, you consider the set of all m by n matrices over the real numbers. So, this is the set of all m by n matrices over the reals. So, what we mean is that all the entries of each and every matrix is real number. So, strictly speaking when we talk about a ring, we mean R m cross n multiplication, addition. Addition is defined component wise multiplication is the usual matrix multiplication.

(Refer Slide Time: 20:46)



So, now let us go back and check which properties are actually satisfied. Is it a commutative ring? No because matrix multiplication is not commutative. Is it a ring with identity? Yes, so you can actually put that down here. It is not a division ring, because a matrix in general does not have an inverse. So, we will put that down here.

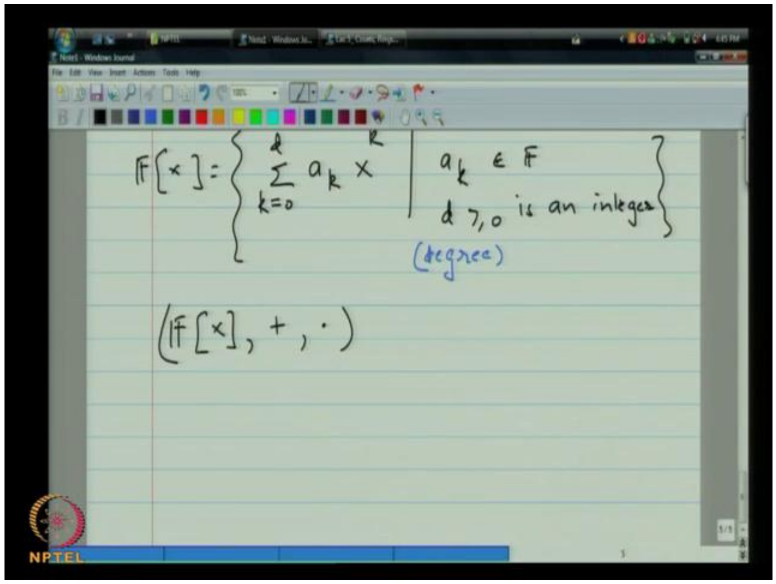
(Refer Slide Time: 21:12)



Next example, we are going to define F rectangular bracket X. This notation denotes the set of all polynomials in the indeterminate X over F. So, another way of expressing this is to say that, this is the set of all expressions of the form summation k goes from 0 to d a sub k X to the k, where the a sub k belong to F and where d greater than or equal to 0 is an integer.

So, this is what we mean by a polynomial in the indeterminate and this d is called the degree, so make a note of that. So, again you have to when you talk of a ring you have to introduce operations.

(Refer Slide Time: 23:25)

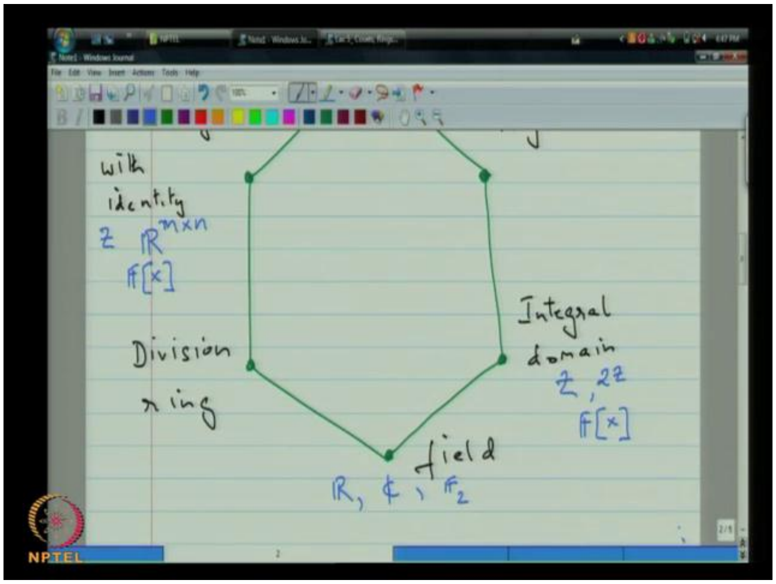


So, we are speaking of F x plus and this. So what do we mean by addition of polynomials? It is the usual addition, if you add you add them component wise and multiplication of polynomial also takes place in the usual way.

So, most of you all are familiar with this so I will not spend time on it. So, let us go back to the interesting question where would you place this here? So, as a ring you can verify it very quickly that is the ring multiplication is commutative. The order in which you multiply 2 polynomials does not make a difference. It is also an integral domain, because if you multiply 2 polynomials, you cannot get 0 unless one or the other is the 0 polynomial.

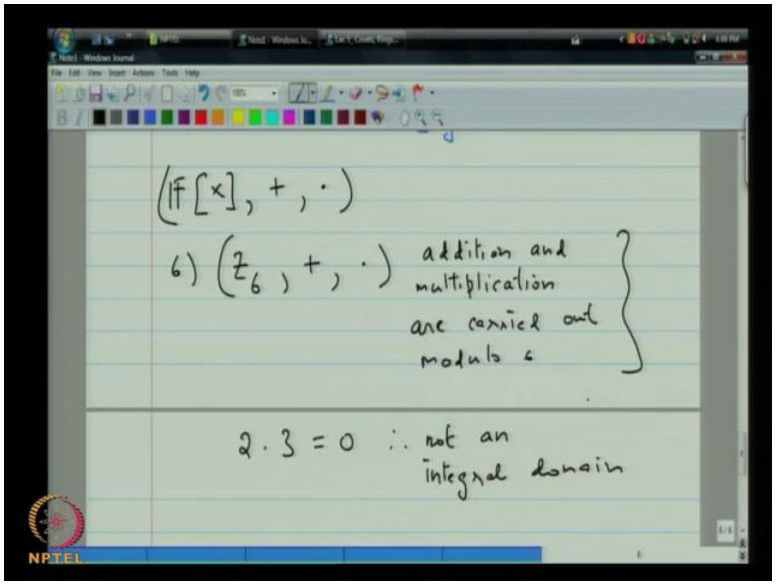
Now, that is not immediately obvious, but if you just sit down for a couple of minutes you should be able to see a way of proving that. Is it a ring with identity? Yes, because the polynomial which is just the constant 1 is the identity. Is it a division ring? No, because for example; the polynomial X does not have an inverse.

(Refer Slide Time: 24:47)



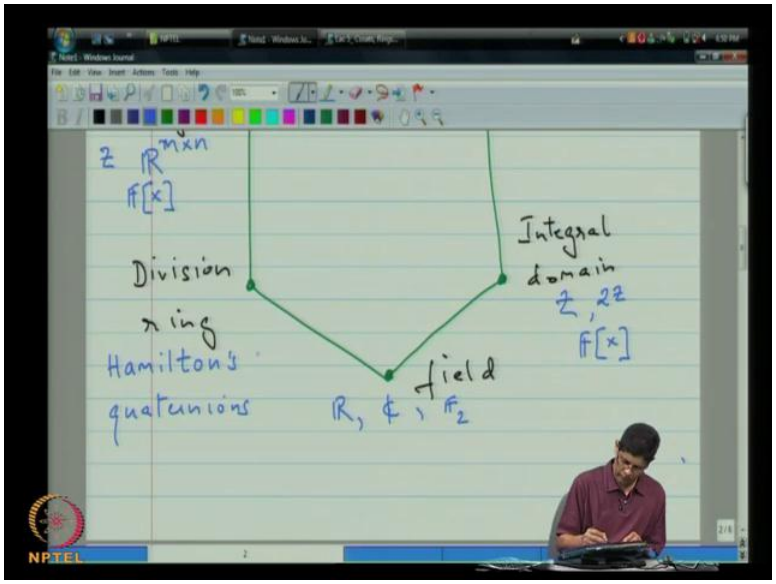
So, here again we would put this here and here. So, we have seen examples. Now, if you look at this figure, there are 2 gaps in some sense. So what could we put in here and here? So in other words we are looking for a commutative ring which is not an integral domain.

(Refer Slide Time: 25:24)



So, this is examples 6 then. So, consider Z 6 under multiplication. So, addition and multiplication take place modulo 6. So, you can check that at the defining axioms of ring are satisfied it is commutative, but it is not an integral domain, but because 2 times 3 is equal to 0. Therefore, it is not an integral domain.

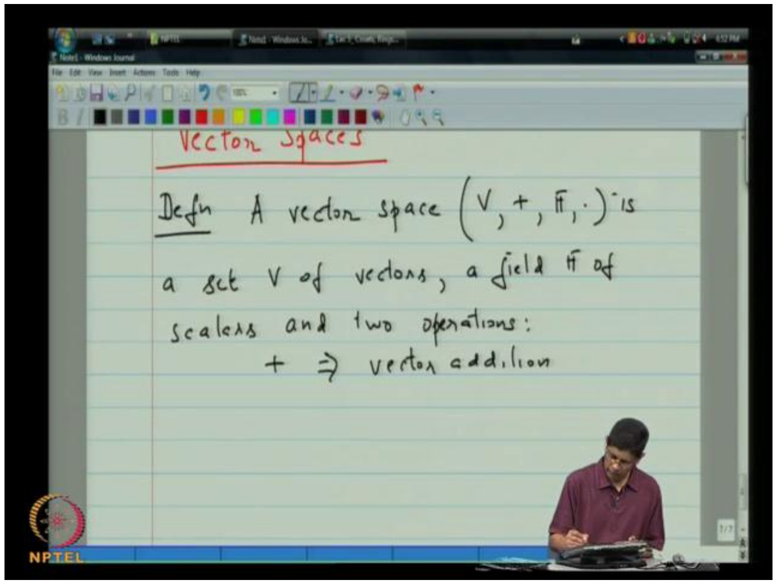
(Refer Slide Time: 24:47)



So, in this figure we can put down here Z 6. So, now we have one entry less to fill which is a division ring that is we are looking for something in which it is a ring, the ring has an identity and every element has an inverse. The only thing that is missing is that multiplication is not commutative.

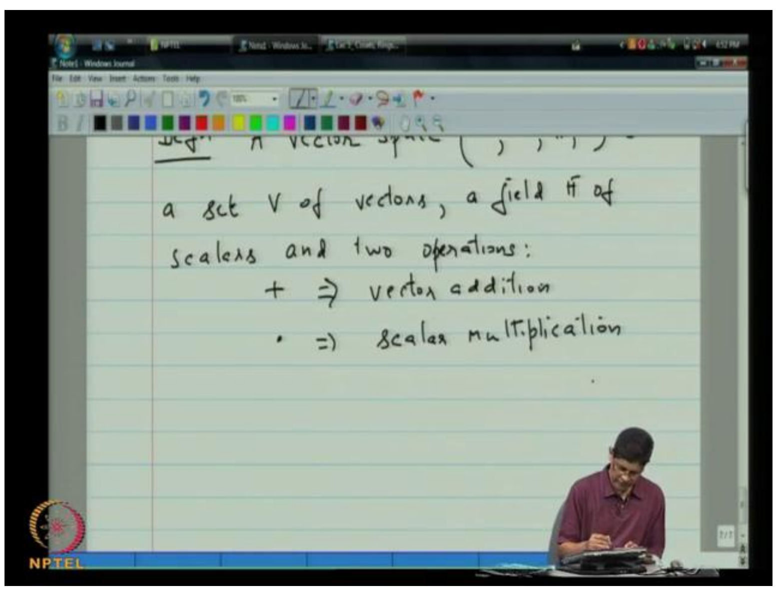
So, I will not actually go through this discussion it will take us too far away from our subject. But an example, of this is Hamilton's quaternion's and it turns out that now this seems like pure mathematics at this point, but it turns out that extensions of Hamilton's quaternions have actually found application in wireless communication. And certain very efficient space time codes for multiple antenna communication have been constructed using objects which are generalizations of the quaternions.

(Refer Slide Time: 28:48)



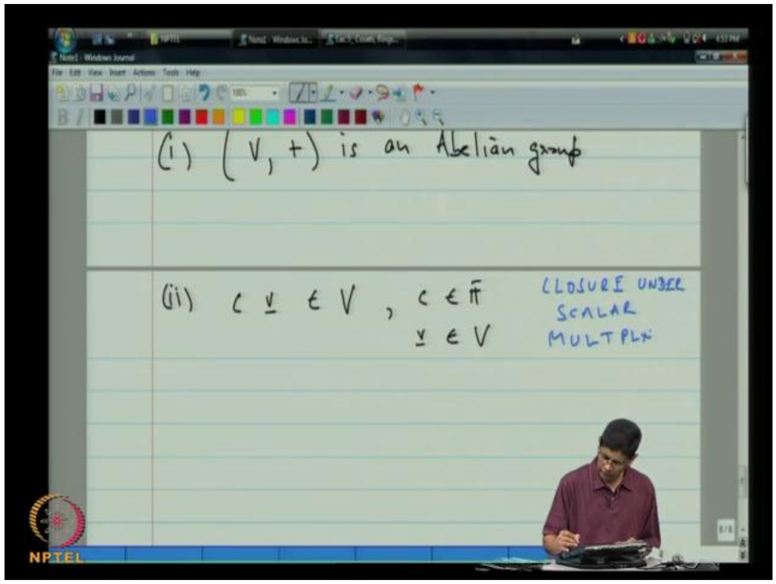
So, with that we are done with the topic of rings and fields. So, now we will move on talking about vector spaces. So, definition a vector space V plus is a set V of vectors a field F of scalars and 2 operations plus, which we will call vector addition.

(Refer Slide Time: 30:11)



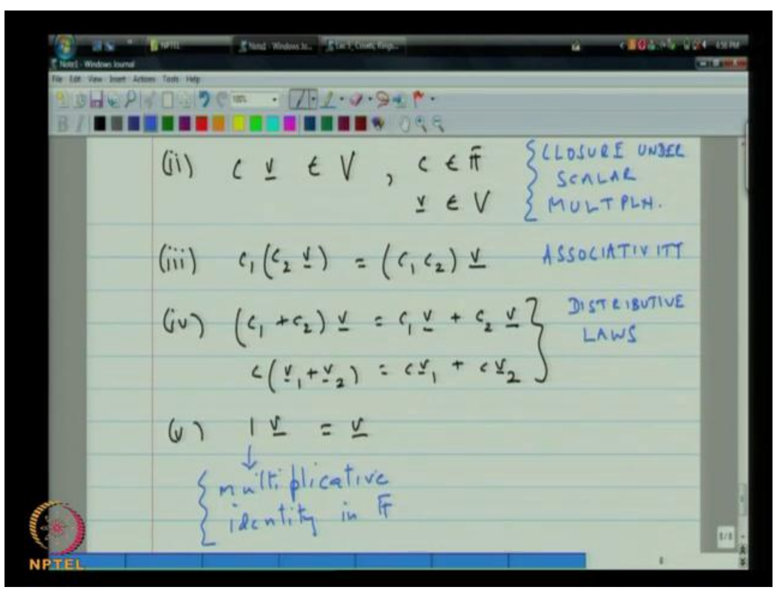
And dot which will be scalar multiplication, such that the following properties hold.

(Refer Slide Time: 30:41)



One: V plus is an Abelian group. Two: C times v is in V for C in F v in V. So, there is a distinction between the capital and the lower case v. So, whenever we introduce a vector we will put a bar underneath it. So, this is the axiom of closure. So this is closure under scalar multiplication.

(Refer Slide Time: 31:58)



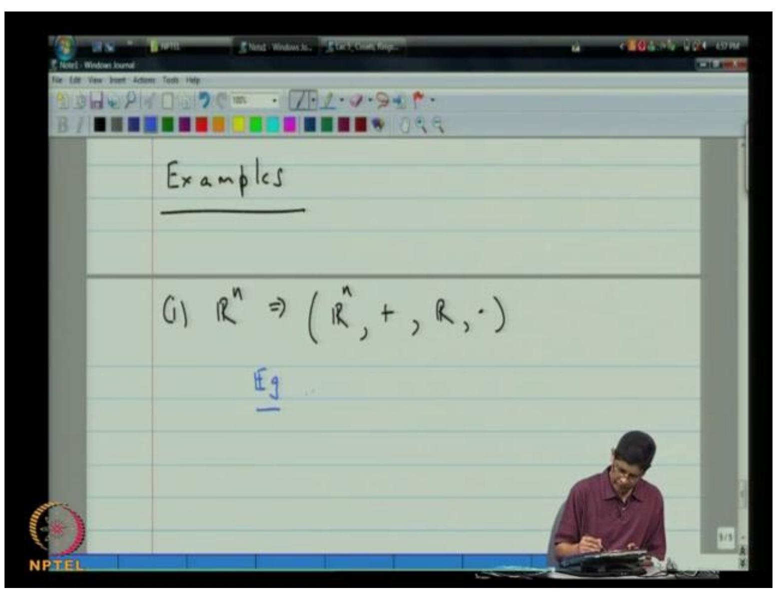
Then, if you take c 1 times c 2 v that is the same as c 1 c 2 times v. So, this is associativity of scalar multiplication. Next you have the distributive laws, which say that c 1 plus c 2 times v is c 1 times v plus c 2 times v and that is c times v 1 plus v 2 is c times v 1 plus c times v 2.

So, these are called distributive laws. The final axiom says that if you take the element 1 and multiply any vector with it you get the vector back. So, this is how all these axioms 2 3 4 and 5 are telling you how the scalars interact with the vectors.

So, one is telling that if you multiply a scalar and a vector, then you will get a vector. This multiplication is associative, it is distributive and if you take the identity element in the field, because we know that the scalars form a fields. So there is a multiplicative identity. If you take the identity element in the field then and multiply into a vector, then that vector will remain unchanged.

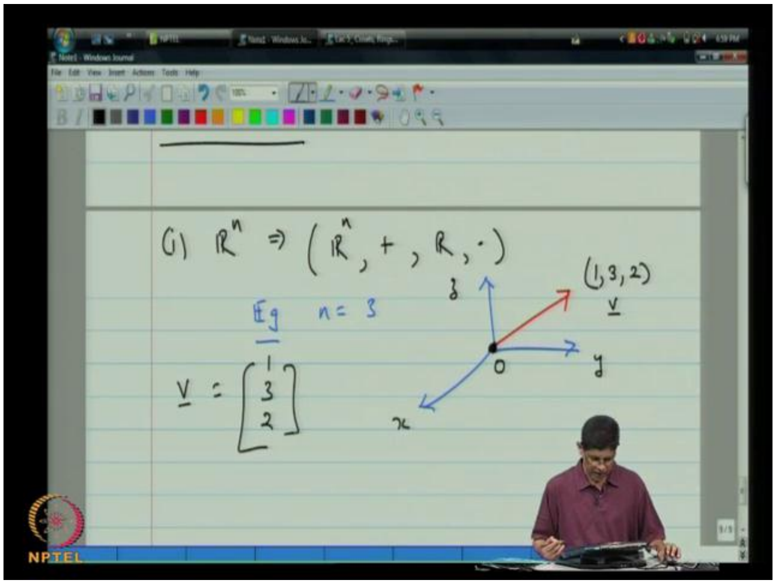
So, it is worth just pointing out here that this is the multiplicative identity. So these are the axioms that go to defining a vector space. So, if you keep in mind that in order for something to be an Abelian group it needs to satisfy 5 condition, this makes for a total of 5 6 7 8 9. So, there are total of 9 conditions that need to be satisfied.

(Refer Slide Time: 35:07)



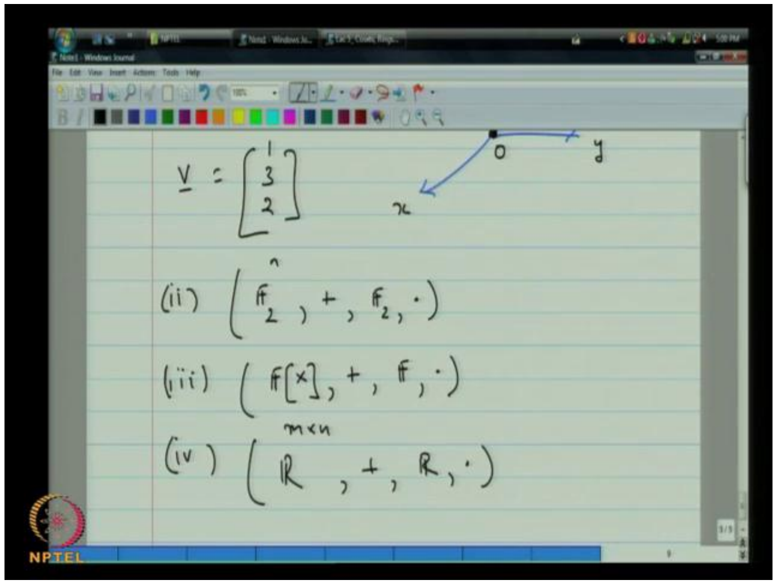
So, what are some examples? The most common examples are vector spaces of the form R to the n, where strictly speaking we mean R to the n is the set of vectors. This is ordinary vector addition, these scalars are the real numbers and you have multiplication.

(Refer Slide Time: 35:54)



So this is an example within an example. So, here if you take n is equal to 3, then you can actually draw a geometric picture. So, a vector would then let us say that, this is the point, this is the origin and let us pretend that this is the point whose coordinates are 1. So, this is the x, the y and the z axis, so 1, 3, and 2. So, then this line here would represent the vector 1, 3, 2. So, you can verify that this forms a vector space.

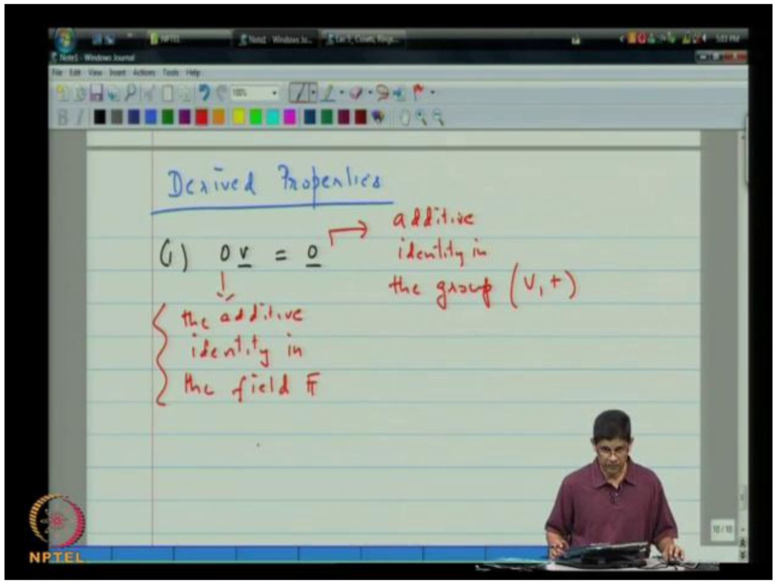
(Refer Slide Time: 37:03).



Similarly, analogously you also have the vector space F 2 to the n addition F 2. This is the analog of the vector space of the real numbers except that you replace the field of real numbers by just the set of all binary n tuples. You can also look at the set of all polynomial over a field, where the field the field defining I mean it is a same field the scalar field is precisely the coefficient field of the set of all polynomials.

And you can even think of the set of all m by n matrices as forming a vector space. Again I think for lack of time, I will not actually bother going through the verification process. I think addition and multiplication the definition in every one of these cases is fairly straight forward. So, you just have to go through the axioms and verify for yourself that they are actually satisfied.

(Refer Slide Time: 39:00)

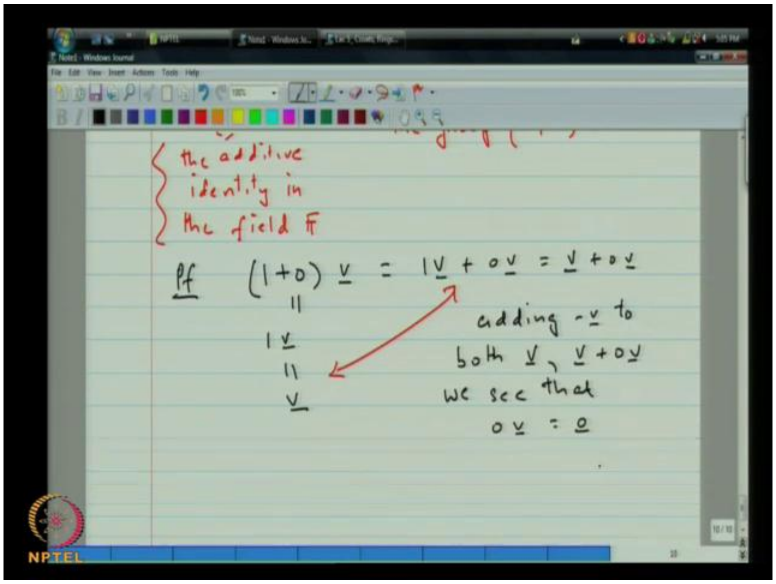


Next we will actually go through some, list some derived properties and I think part of the reason for going through with this is, because whenever you think of a vector space, there will be a temptation on your part to actually think of a particular vector space. Perhaps 3 dimension space or 4 dimension space, but sometimes you need to get away from that and think only in terms of the axiom.

So, you have to just think very logically and not fix your mind on any particular example of a vector space. So, in going through a proof of some of these derived properties it will turn out that that the processes in exercise and thinking along those lines. So, one of the derived properties states that, if you take if you take 0, and multiply a vector with it, you will get the 0 vector, so what is 0 here mean? This 0 is the additive is the additive identity in the group V plus. On the other hand this 0 here is the 0, the additive identity in F or more precisely in the field F in the field F.

So, the two 0(s) are different and now, we are saying something about how they interact. We are going to say that, if you take the scalar 0 multiply into a vector then you will get the vector 0. Now, if you are seeing this for the first time you will say that is obvious. It is kind of stupid trying to prove that. But that may be because you are fixing your mind on a particular vector space.

(Refer Slide Time: 41:38)

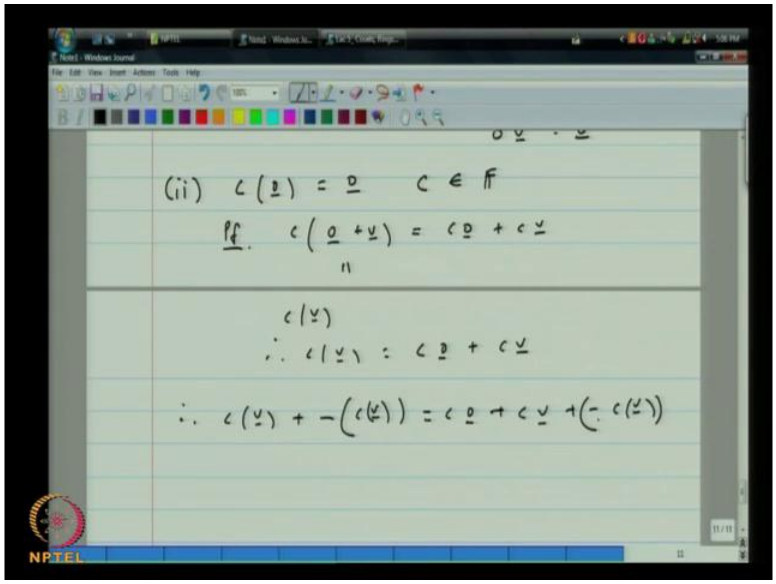


Here, we are saying we want to prove it for all vectors spaces. So, we need to work only with axioms. So, the proof of this will proceed like this. If you take 1 plus 0 times v, then this will be 1 times v plus 0 times v. On the other hand, this is 1 times v because 1 plus 0 is 1 which we know from an axiom is equal to v.

So now, we compare we compare the two and we see that by the way even here I can this little bit further and say that this is v plus 0 times v. So, now adding minus v to both this expression as well as this to both v v plus 0 we see that 0 times v is equal to 0.

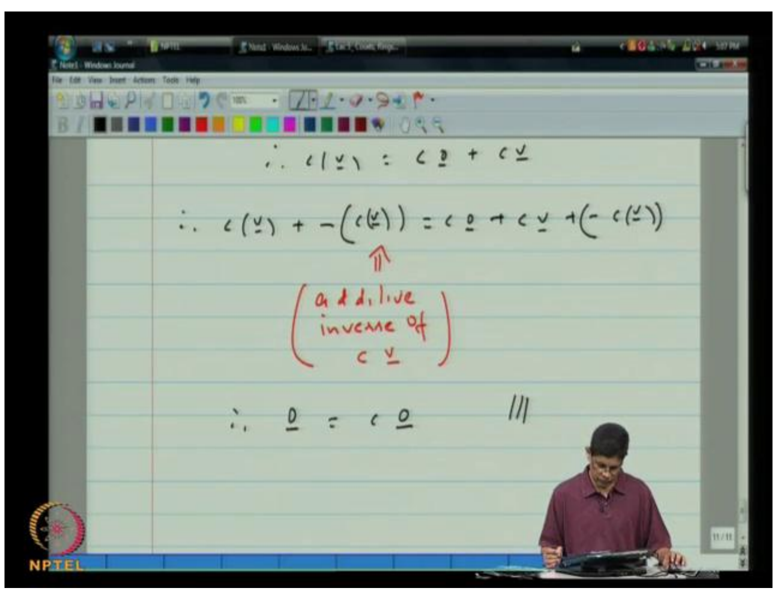
So, this is typically how proofs of this kind will proceed. So, in the interest of moving quickly, I will move quickly through the proofs of the other properties.

(Refer Slide Time: 43:14)



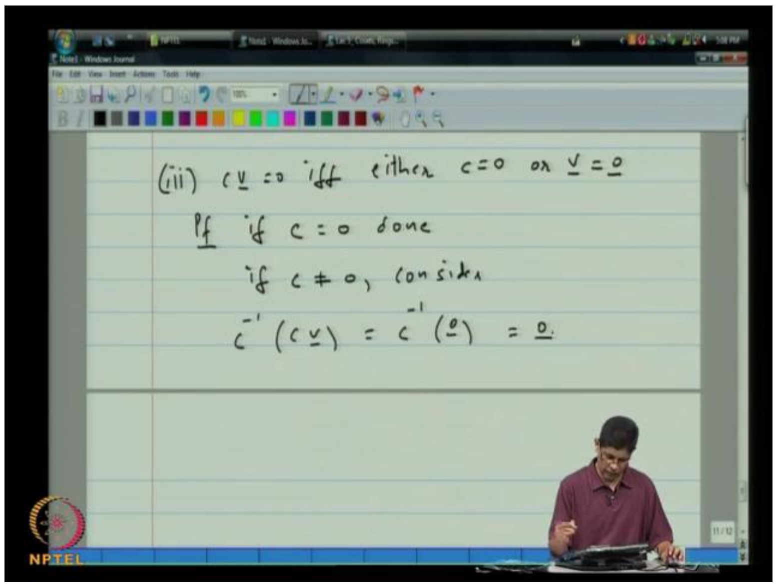
If you take if you take c times 0 vector for any scalar, then you will recover the 0 vector. So, how do you prove that? c times 0 plus v is on the one hand c times 0 plus c times v. On the other hand that is c times v. Therefore, c v is c 0 plus c v. So, what we can do is we can add the additive inverse of c v on both sides. Therefore, c times v plus the additive inverse of c times v is equal to c times 0 plus c times v plus minus of c times v.

(Refer Slide Time: 44:36)



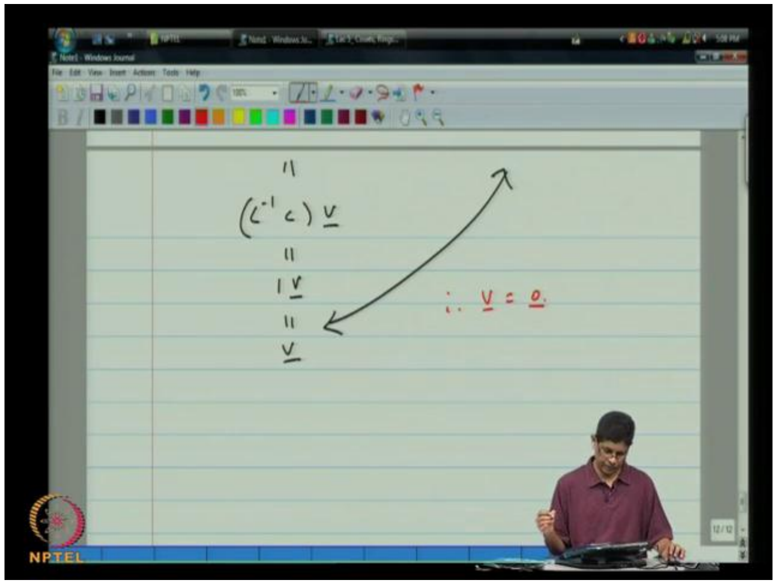
So, you should read this as the additive inverse of c times v. And now of course, this gives you zero vector on the left, because you take any element and add its inverse you will get the identity. Therefore, 0 is equal to c times 0 and we are done with that proof. So, to summarize what we have shown is that c times the vector zero is 0 and we also showed that the scalar zero times any vector is 0.

(Refer Slide Time: 45:26)



Now, the third property says c times v is equal to 0 if and only if either c equal to 0 or v equal to 0. So, proof: if c equal to 0 we are done. If is c is not equal to 0 if c is not equal to 0, then consider c inverse times c v which is equal to c inverse times 0. But we know that any scalar that multiplies 0 will give us 0. That was what we just proved.

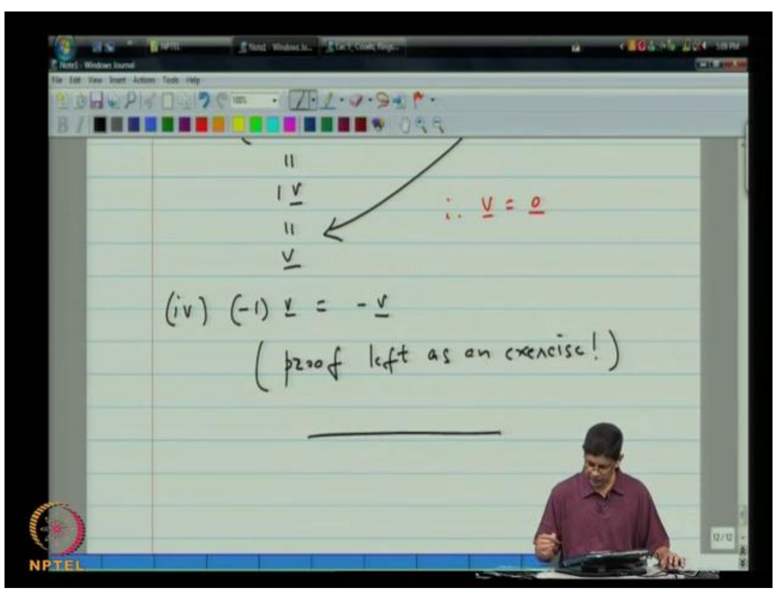
(Refer Slide Time: 42:26)



But, on the other hand this is c inverse times c times v which is equal to one times v, which is equal to v. So, now you compare these two and conclude therefore, that v is equal to 0.

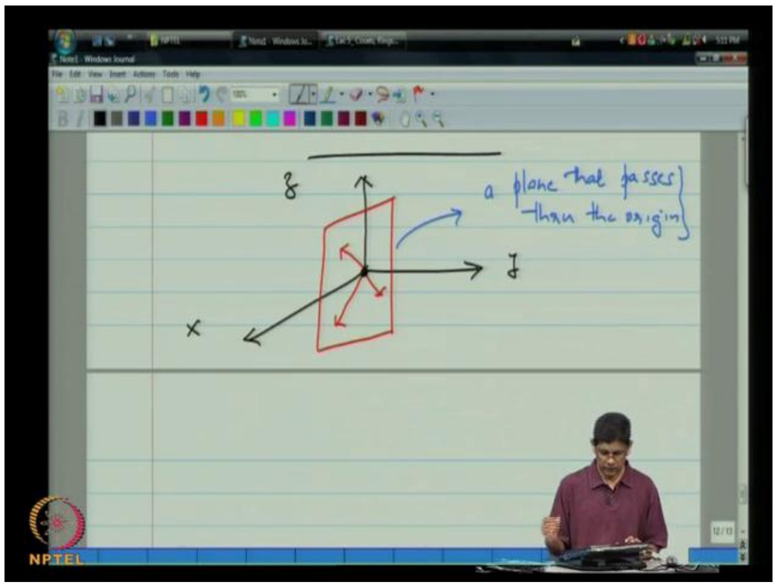
So, I am going through these a little bit fast. But I am going to assume that you will have some time to look through the notes on your own after words and make sure that you understand the proofs.

(Refer Slide Time: 47:13)



Then, as an exercise you can try to prove that minus 1 times v is equal to minus v. So, that is something that you might want to try to prove on your own. So, we are done with derived properties. Now, what we want to do is look at instances, when a larger vector space contains a smaller vector space.

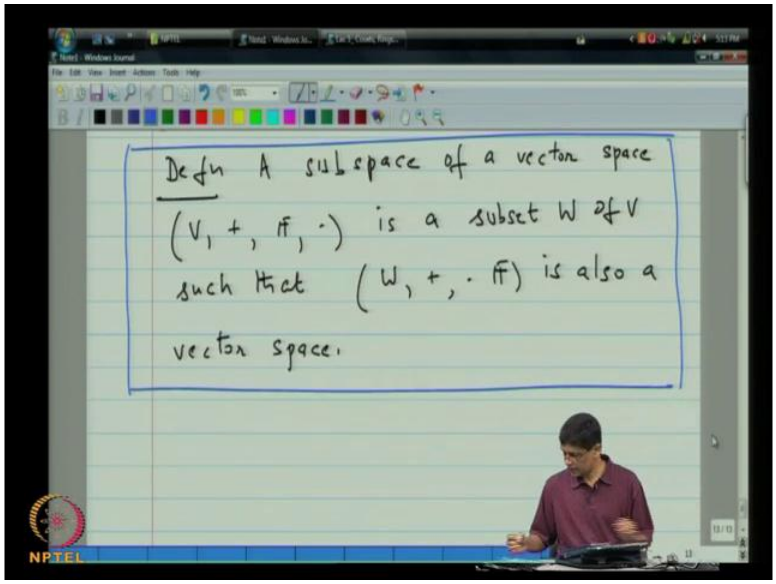
(Refer Slide Time: 48:07)



So, I will illustrate with a picture. So, supposing you have something like this and then you have. And let us say that this thing here is a plane that passes through the origin. So in this case, it turns out that this plane is sitting inside 3 dimension space, which is the vector space. It turns out that the elements in the plane also by the way when I draw this plane I mean an infinite plane. So, this diagram in that sense is misleading. So, there is no limit it is the infinite plane.

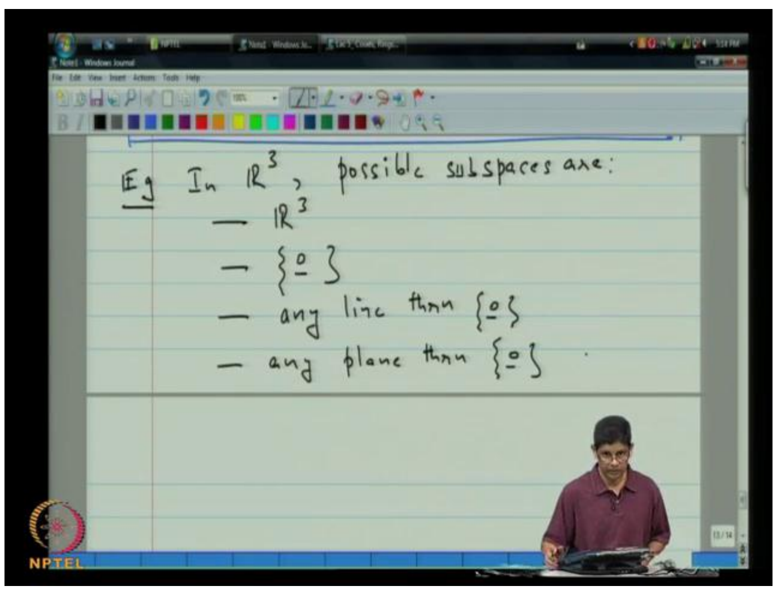
So, if you consider all vectors in the plane such as, for example this. So, I mean that this plane for example, includes vectors like this, vectors like this, vectors like this, and these vectors could have infinite length. So, then this is also a vector space. So, when you have one vector space sitting inside another the smaller vector space is called a sub space. So that is our next topic.

(Refer Slide Time: 49:46)



A subspace of a vector space is a subset W of V such that W plus dot F is also a vector space.

(Refer Slide Time: 51:17).

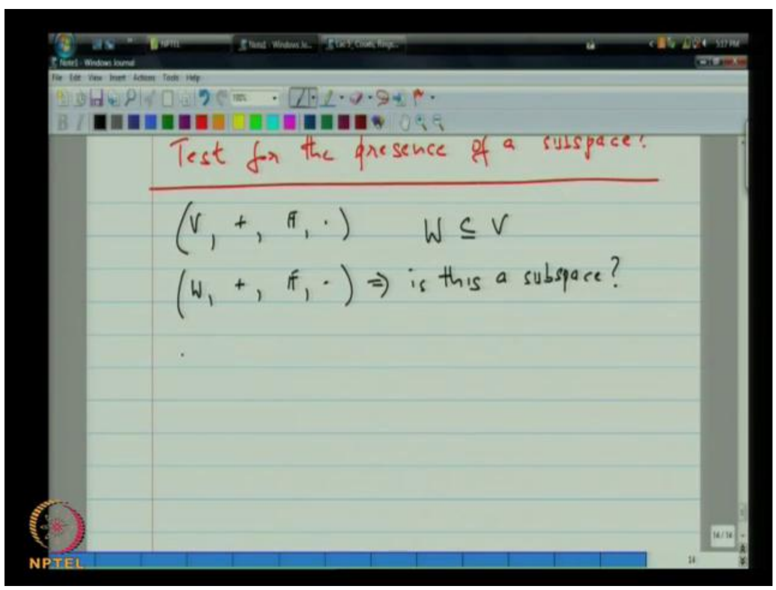


So, what are some examples? In R 3, that is in three-dimensional space, possible subspaces are one: R 3 all of R 3 just the origin, any line through the origin, any plane through the origin. So, these are the only possible subspaces of three-dimensional space. Now, just looking ahead a little bit you can explain why there are only these kinds of subspaces, because later on we will attach a measure to a subspace and that measure is called dimension.

Now, R 3 in everyday language called three dimension spaces, but in a very formal mathematical sense it is an algebraic object that has a dimension of 3. To the subspaces also you can ascribe dimensions. So, each of the three four items that we have listed below corresponds to a different dimension. So, R 3 is three dimensional the 0 vector is of dimension 0, any line is dimension 1, any plane is dimension two.

So, that is why these are the only kinds of sub spaces. Again I am going to leave it you to verify that, they are actually indeed subspaces.

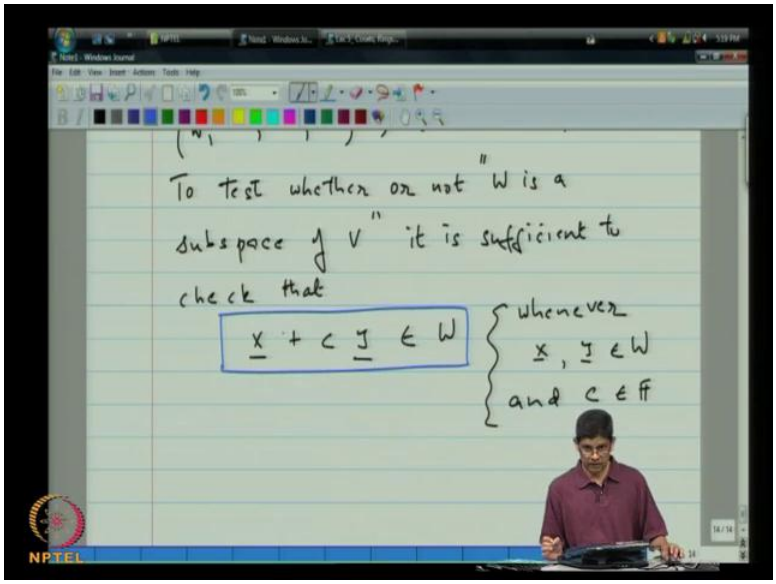
(Refer Slide Time: 53:40)



The next topic is how do you test for the presence of a subspace? So, were in the setting where you have V plus F dot, and then you have W plus F dot and W is given to be a subset of V. And you have given that this is the vector space and you want to test is this a subspace. So, that is your goal.

Now, one way of testing whether something is a subspace is to actually go through all the axioms and as I pointed out earlier there are 9 of them. But that that is the brute force (( )) it turns out just like along using an argument very similar to the argument that we used in the case of groups. You can show that you can actually reduce it to a single test.

(Refer Slide Time: 55:19)



Suffices to test turns out to test whether or not W is a subspace of V. So, let me just put this in quotes because strictly speaking it is not W that is a subspace it is this entire W plus F dot. But that is too long to say so we will just say that we will abbreviate it to W is a subspace of V.

It is sufficient to check that a I am going to use different letter to check that X plus C y is in W. Whenever, X and y belong to W and C is any scalar that belongs to the field of scalars. So, you just can apply this one test and that in a sense covers all the 9 axioms. Why is that? So, if you ask the question how does this cover all the axioms.