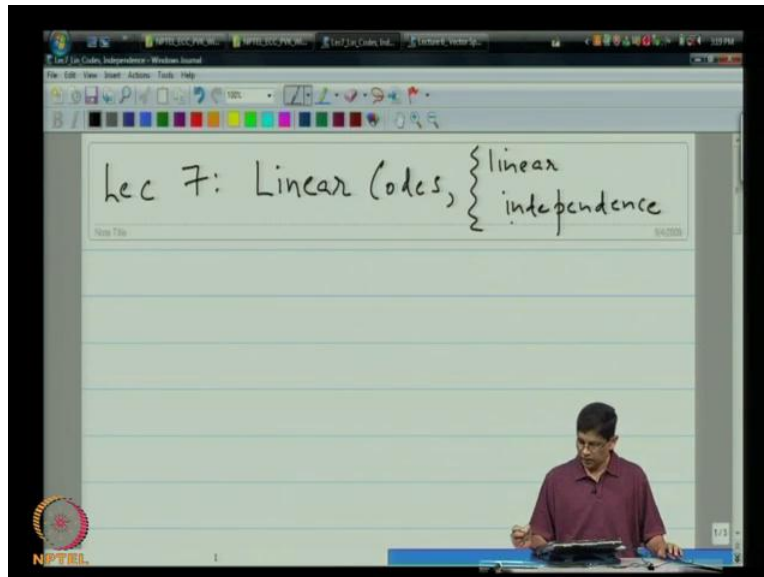


**Error Correcting Codes**  
**Prof. Dr. P.Vijay Kumar**  
**Department of Electrical Communication Engineering**  
**Indian Institute of Science, Bangalore**

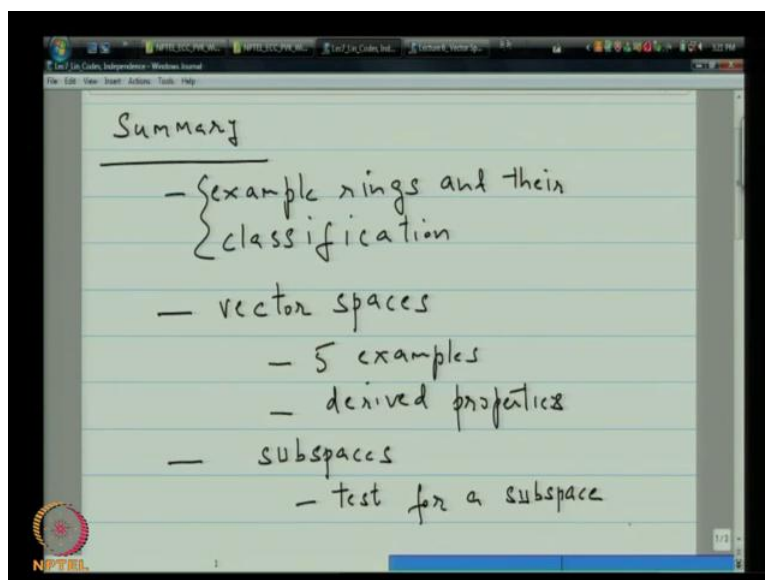
**Lecture No. # 07**  
**Linear codes and Linear independence**

(Refer Slide Time: 00:30)



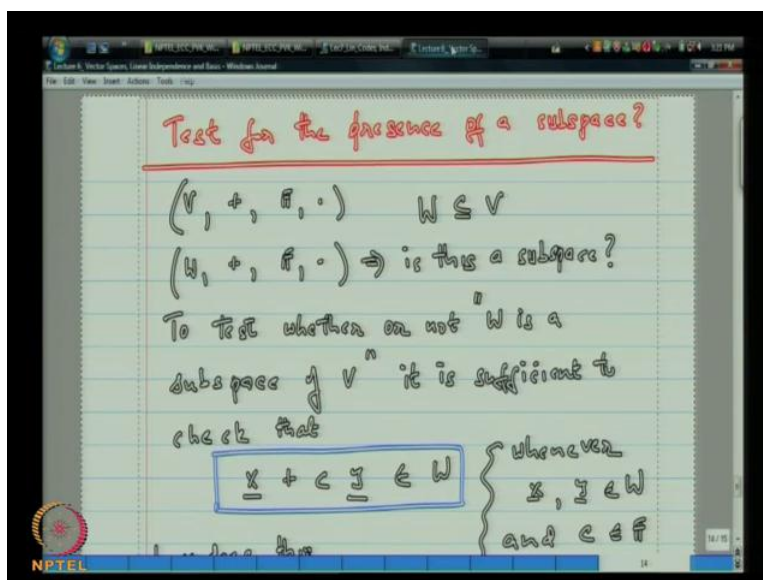
Welcome to the this is seventh lecture in our series, let me put down the title. Now, in the last lecture I was instructed by the operators here to write a little bit bigger. So, I am going to try to stay with slightly bigger print today, and see how that works out. So, let me begin with the title is linear codes and linear independence.

(Refer Slide Time: 01:19)



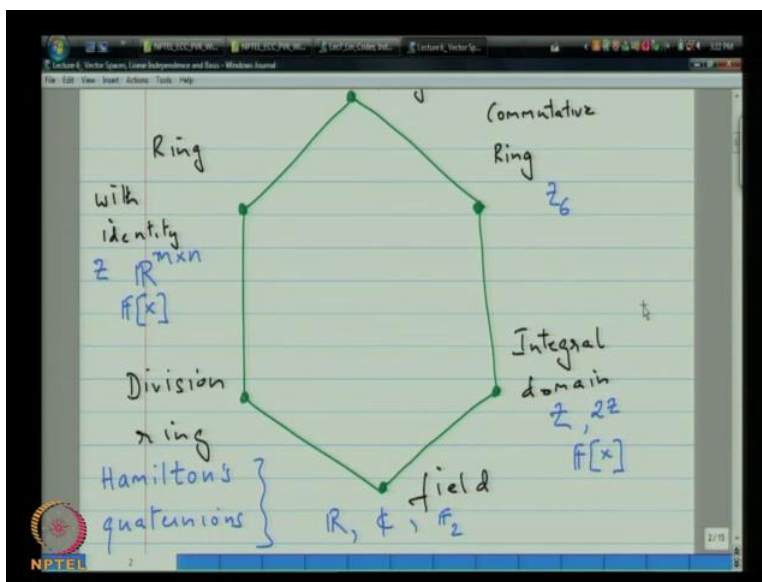
I will begin with summary of what we did last time. So, we looked at example: rings and their classification. Then we moved on to a different example of an algebraic structure which was vector spaces, here we looked at five examples, and we looked at derived properties. Then towards the end of the lecture we started talking about subspaces.

(Refer Slide Time: 03:09)



And we talked about how one would go about test testing for the presence of subspace. Before we get to that let me just go back to our previous lecture, we will quickly browse through it.

(Refer Slide Time: 03:18)



So, here is the part where we are talking about different types of rings and their classification, where you see the light blue those are the example rings that we classified.

(Refer Slide Time: 03:30)

$F_2 = \{0, 1\}$  field  $(F_2, +, \cdot)$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

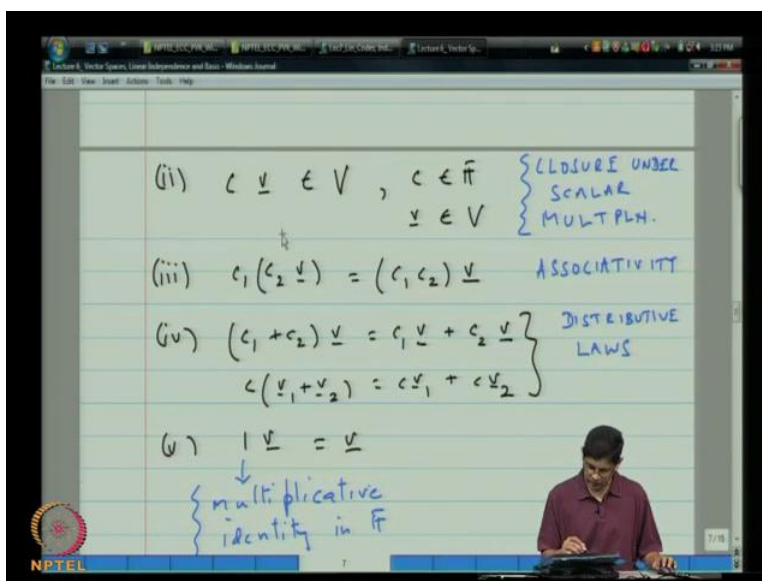
can verify that the set  $\{0, 1\}$  along with the operations defined as above forms a field.

I expanded little bit on the finite field of two elements. Because we will be using this structure very often and there you have the five examples, actually a sixth as well. And then after that we went on talking about vector spaces where, I defined what it was meant what is meant by a vector space and I am going to dwell on this for just the minute.

Because, when we talk about subspaces I will make a reference to these axioms. So, in order for an algebraic structure to be a vector space you need to satisfy basically 9 axioms and you can clump 5 of them together by the just saying that, the collection of vectors together with addition forms an Abelian group.

So, that in some senses is the compact way of stating 5 axioms all together that once, and then that is followed by four other axioms having to do with scalar multiplication and the interaction with vectors.

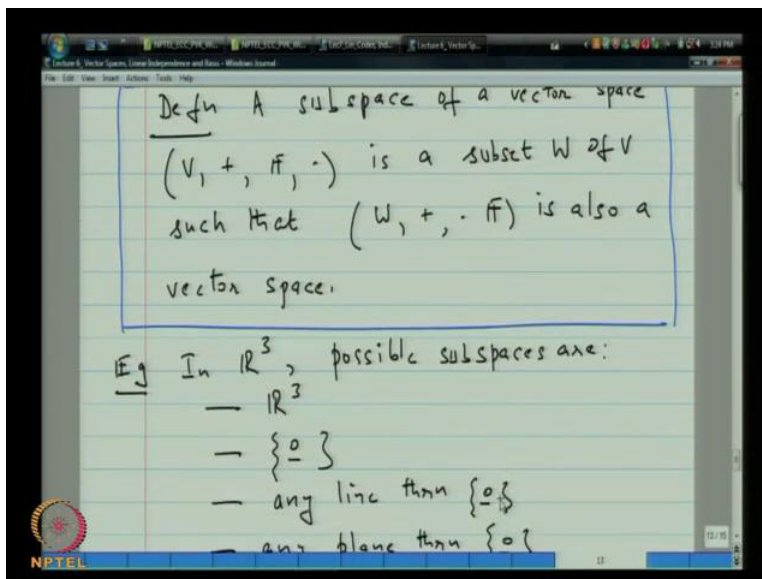
(Refer Slide Time: 04:32)



And those axioms are closure under scalar multiplication, associativity scalar multiplication the two distributive laws that is that scalar addition distributes over vector multiplication and so on. And then finally, that if you take the identity element in the ring and multiply it in the field and multiply it to the vector you can the vector back itself.

So 9 axioms we looked at examples; these are examples in three dimensional space. We looked at some other examples as well. Derived properties, then we talked about subspaces and I defined what is meant by a subspace.

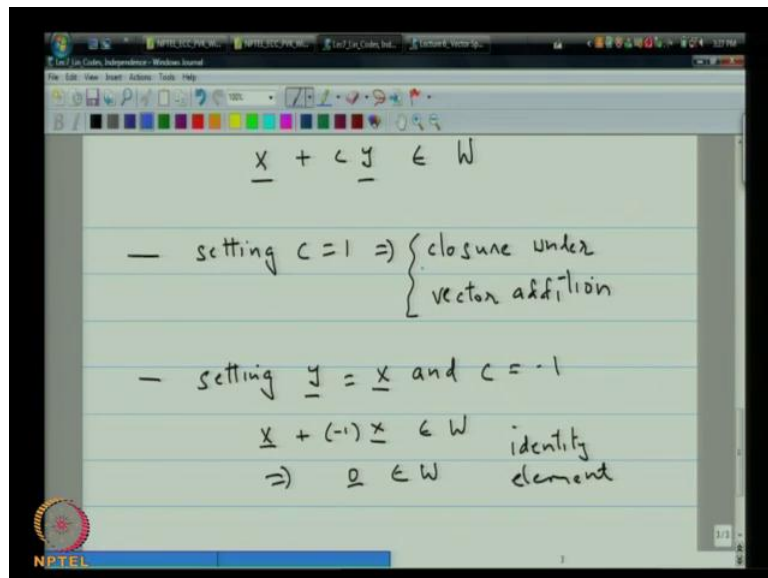
(Refer Slide Time: 05:26)



So, a subspace is a subset that by itself is also vector space. And we looked at examples of subspaces. Now, it is possible that towards end of the last lecture they may have been somewhat abrupt cut off. So, I am going to pick up from this point onwards and we will talk about the test for the presence of a subspace.

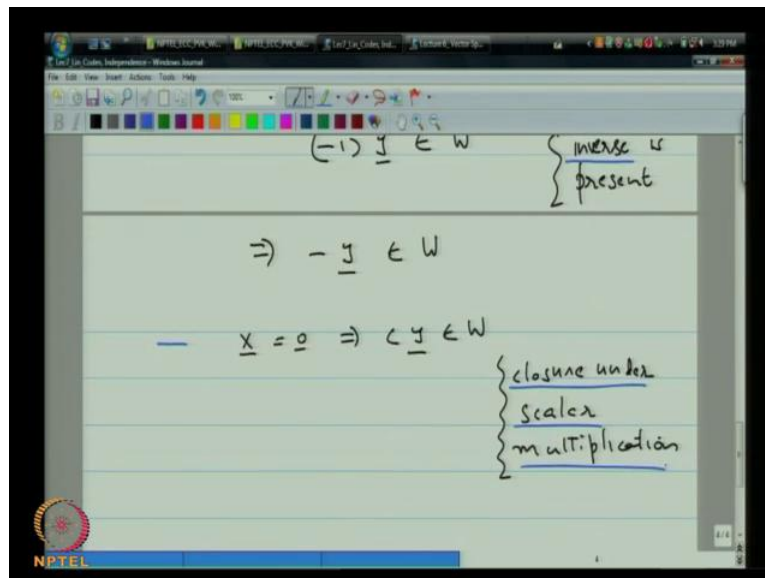
So, here the situation is where you have a vector space and then you have a subset of  $V$  which we will call  $W$ . And the question is  $W$  under the same operations is the also a subspace? Now, of course what you could do is order to test for the presence of a subspace you could go back to all the 9 axioms and verify them individually, but that is time consuming. So, this test that is written down over here namely the test that says that, if  $x$  and  $y$  that whenever,  $x$  and  $y$  belong to  $W$  and whenever,  $c$  is the scalar that belongs to the field. If you could ensure that  $x$  plus  $c y$  is in  $W$  then that is the sufficient and necessary test.

(Refer Slide Time: 07:08)



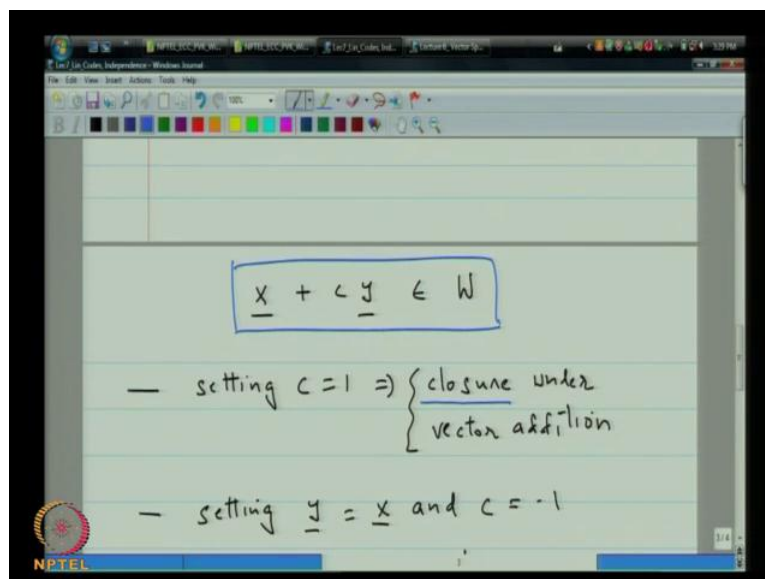
So let us, just see why that is both necessary and sufficient. So, at the top I am going to repeat the test here, first let me just pull up some tool bars that I will be using throughout this lecture. So, the test is that  $x$  plus  $c$  times  $y$  must belong to  $W$ . And the reason why this test suffices is because one: setting  $c$  equals 1 ensures closure under addition, under vector addition. Then next setting equal to  $x$  and  $c$  equal to minus  $y$  ensures that  $x$  plus minus 1 times  $x$  belongs to  $W$  which is to say that  $0$  belongs to  $W$ . So, that ensures that the identity element belongs. So, let me just highlight these in blue. So, you have closure and here you verified presence of the identity element.

(Refer Slide Time: 09:42)



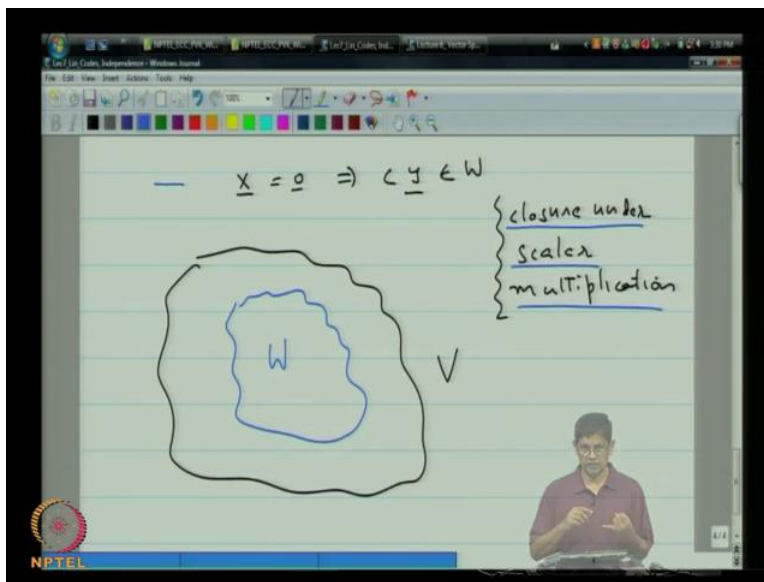
Setting  $x$  equal to 0  $c$  equal to minus 1 ensures that minus 1 times  $y$  belongs to  $W$ , which is equivalent to saying that, minus of  $y$  belongs to  $W$ . So, that is verifying the presence of the inverse and lastly checking that setting  $x$  to be 0 ensures that,  $c$  times  $y$  belongs to  $W$ . So, this is verifying closure under scalar multiplication.

(Refer Slide Time: 10:42)



So, in this way we have ensured that this single test over here is able to take care of four of the tests.

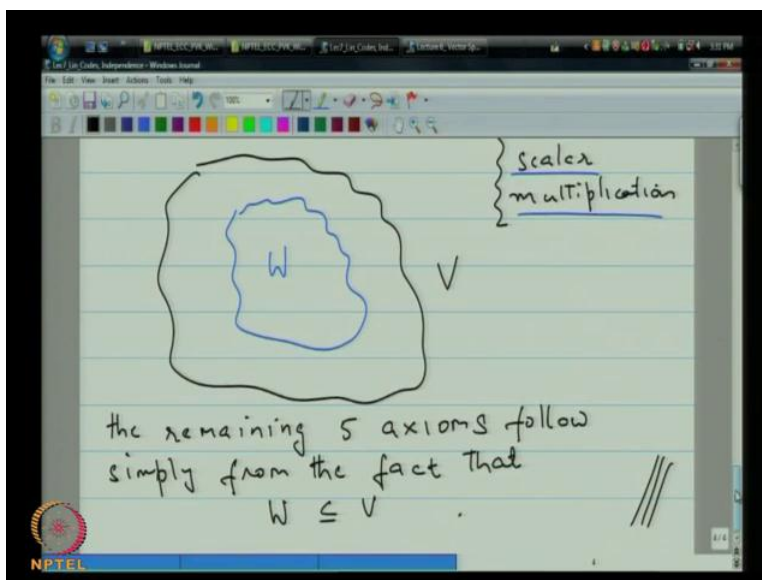
(Refer Slide Time: 11:00)



Now, there are five others that remain but it is straight forward that to note that simply because you have the following situation, where you have collection of vectors, and then you have a subset sitting inside that is  $W$ . So, the axioms for example like associativity under addition, then commutativity under addition, then associativity under scalar multiplication, distributive property of scalar multiplication, and the action of the identity of element. These five other properties follow just from the fact that  $W$  is the subset of  $V$ . So, there is no verification needed.

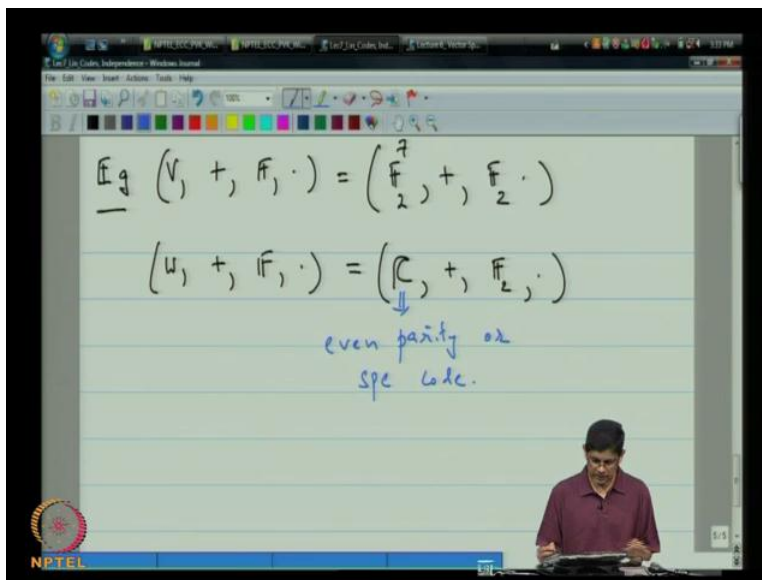


(Refer Slide Time: 11:47)



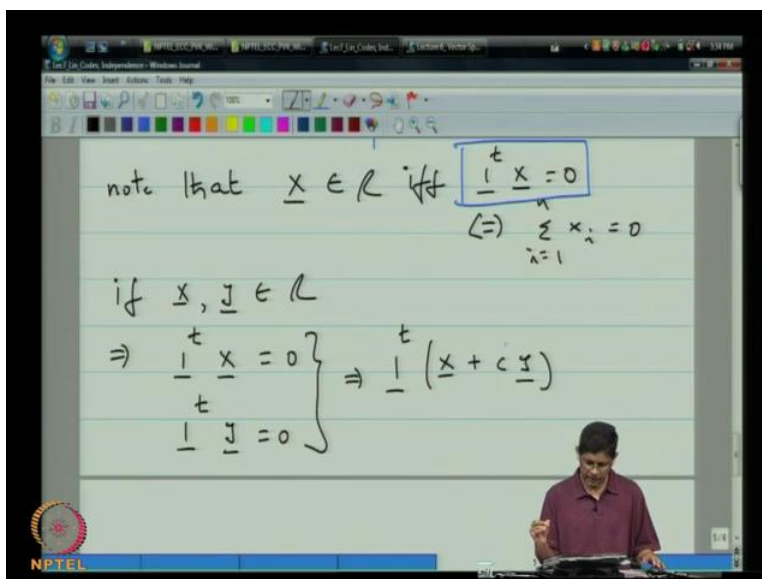
So I will just make a quick note here. The remaining 5 axioms follow simply from the fact that  $W$  is a subset of  $V$ . So, that proves that the single test is all that you need in order to ensure that you have a subspace let us, apply that in an example.

(Refer Slide Time: 12:41)



Let us, say that your parent vector space that is  $V$  plus  $F$  dot is  $F^2$  to the 7 plus  $F^2$  dot and that the subset that you are intending to test is a code, and the particular code that I want to test here is the even the even parity or the single parity check code.

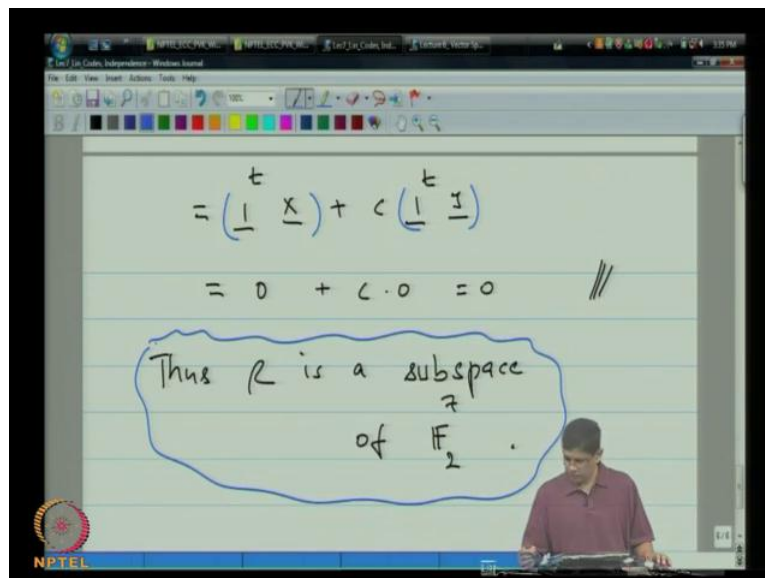
(Refer Slide Time: 14:03)



So, I would like to show you that, this is a subspace. Now, there is simple way to do it. And that is to say that, note: that  $x$  belongs to  $C$  if and only if  $1^t x$  is equal to 0, which is the same as saying that  $\sum x_i$  is equal to 0. So, we will actually use this equation here.

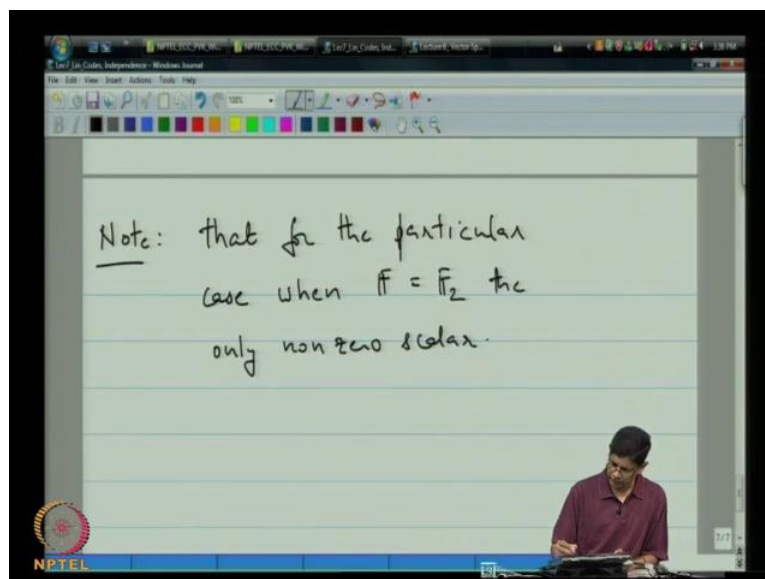
And so now, if  $x$  and  $y$  belong to  $C$ , then that implies that  $1^t x$  is equal to 0,  $1^t y$  is equal to 0.

(Refer Slide Time: 15:09)



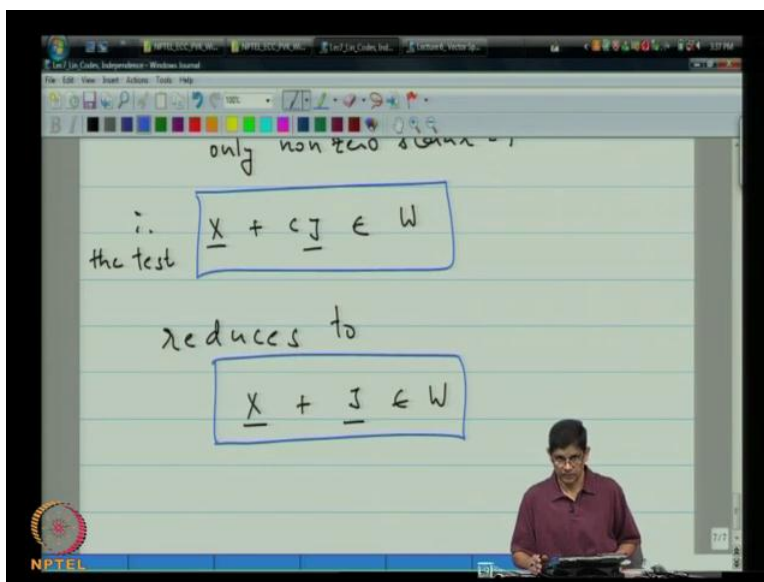
But together this imply that  $1$  transpose  $x$  plus  $c$   $y$  is equal to  $1$  transpose  $x$  plus  $C$  times  $1$  transpose  $y$  and now, you know that individually these two terms are  $0$ . So, this is  $0$  plus  $C$  times  $0$ , excuse me these are scalars. This is  $0$  plus  $c$  times  $0$  which is  $0$ , so you are done. So that ensures that, you have subspace. Thus, the even parity code is the subspace  $\mathbb{F}_2^7$ .

(Refer Slide Time: 16:23)



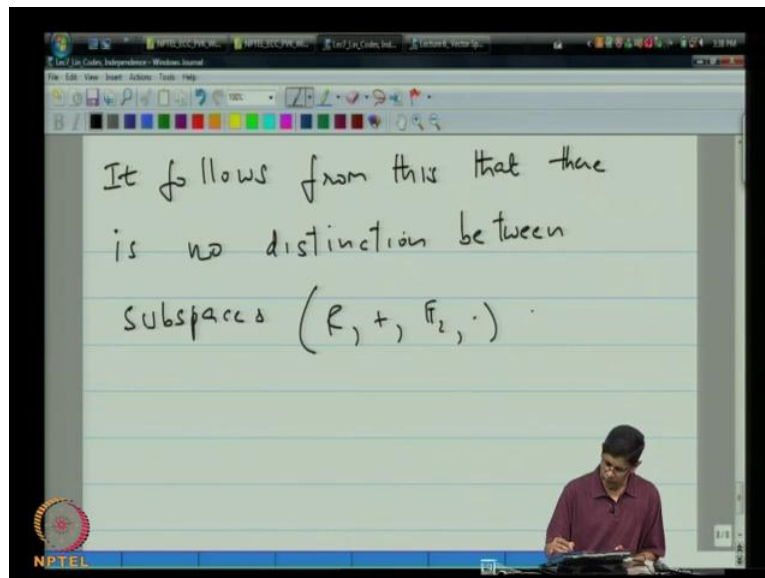
I want to point out something here. Note that for the particular case when,  $F$  is  $F_2$  the only non zero scalar is equal to 1.

(Refer Slide Time: 17:00)

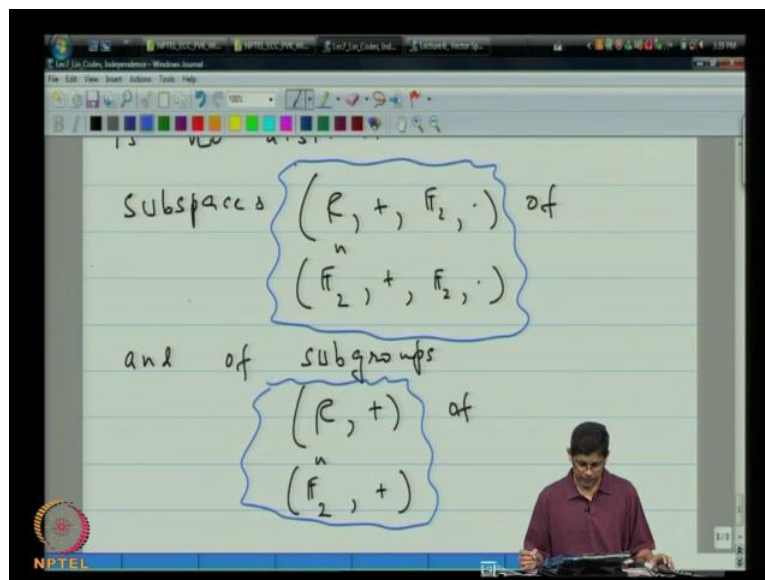


Therefore, the test  $x$  plus  $c y$  in  $W$ , so let me say the test  $x$  plus  $c y$  in  $W$  reduces to  $x$  plus  $y$  is in  $W$ . So now the coding theory examples, where the field is just the field of two elements, because  $c$  the  $c$  over, here that appears here is the scalar. And there are only there is only one nonzero scalar here. So, the test simplifies to this. And now, if you go back in your notes and look you will notice that when we tested for the presence of a subgroup of  $F_2$  to the 7 we had the same test. Therefore, there is no distinction between subspaces of  $F_2$  to the  $n$  and subgroups.

(Refer Slide Time: 18:20)

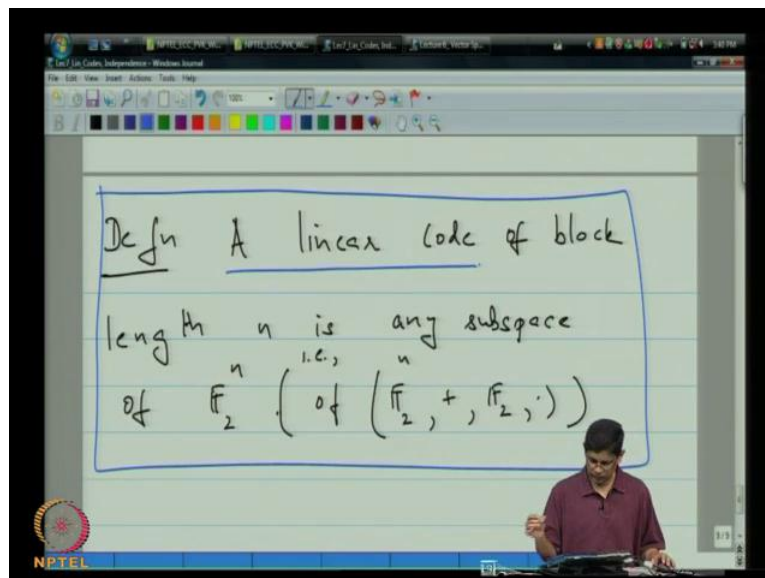


(Refer Slide Time: 19:05)



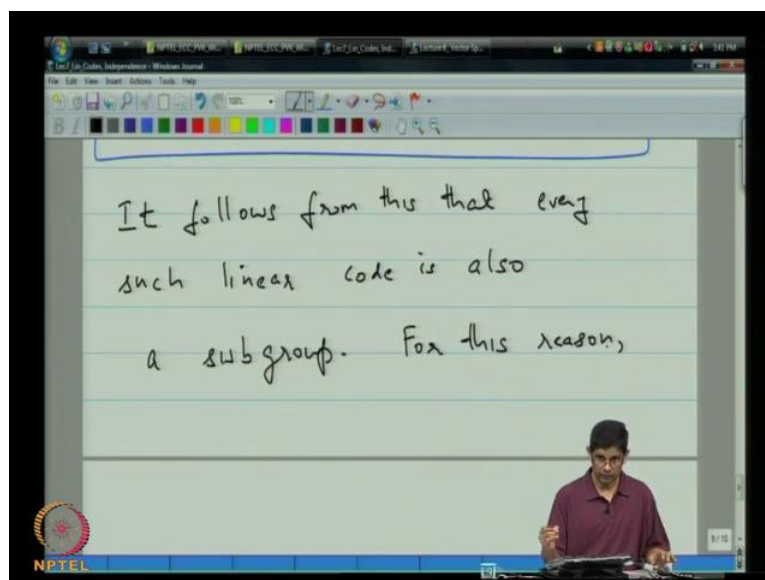
So, it follows from this that there is no distinction between subspaces of the set of  $n$  tuples over  $\mathbb{F}_2$  and of subgroups. So, in other words whether, you are testing to see if particular code is the subspace of the set of all  $n$  tuples or you are just checking to see if it is a sub group of the set of all  $n$  tuples, if you would use an additive sub group the test is the same.

(Refer Slide Time: 20:23)

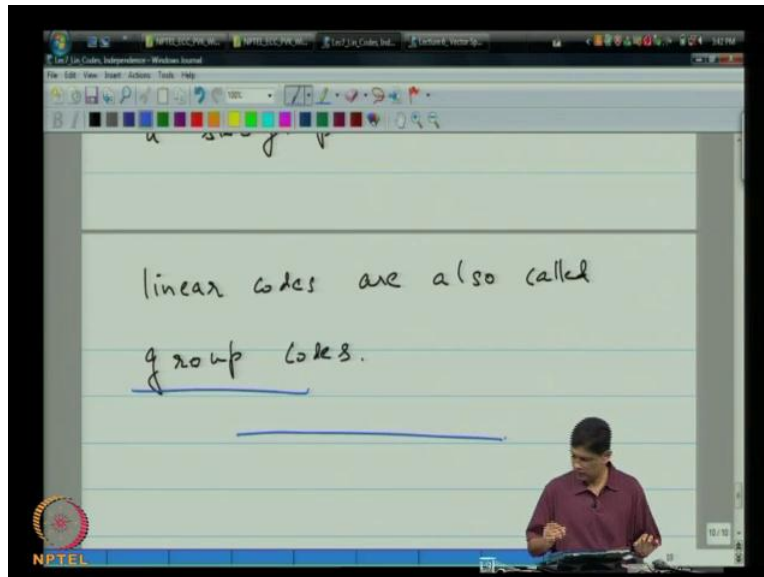


And now for a brief movement we will return to error correcting codes and we will make definition; a linear code of block length  $n$  is any subspace of  $F_2^n$ . And when we say, of  $F_2^n$  we really mean of  $F_2^n$  plus  $F_2$  dot.

(Refer Slide time: 21:41)

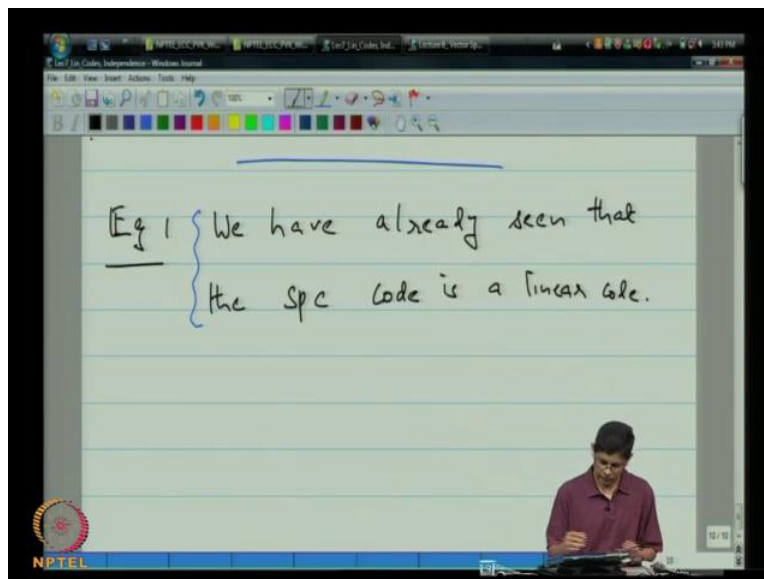


(Refer Slide Time: 22:32)



It follows from this, that every linear code is also a subgroup. For this reason, linear codes are also called group codes. So, that is just a quick remark.

(Refer Slide Time: 23:11)

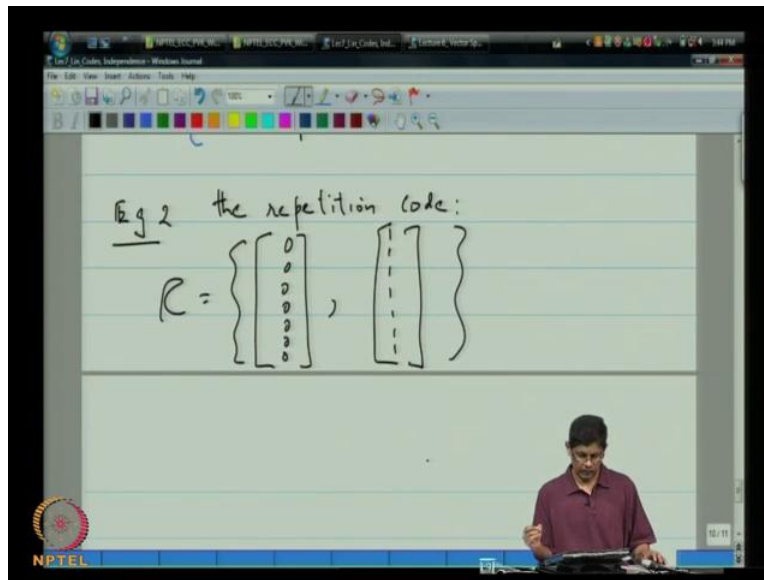


Now, as far as examples go we have already seen we have already seen that, the single parity check code is a linear code. Simply, because what we did was we verified that it is a subspace



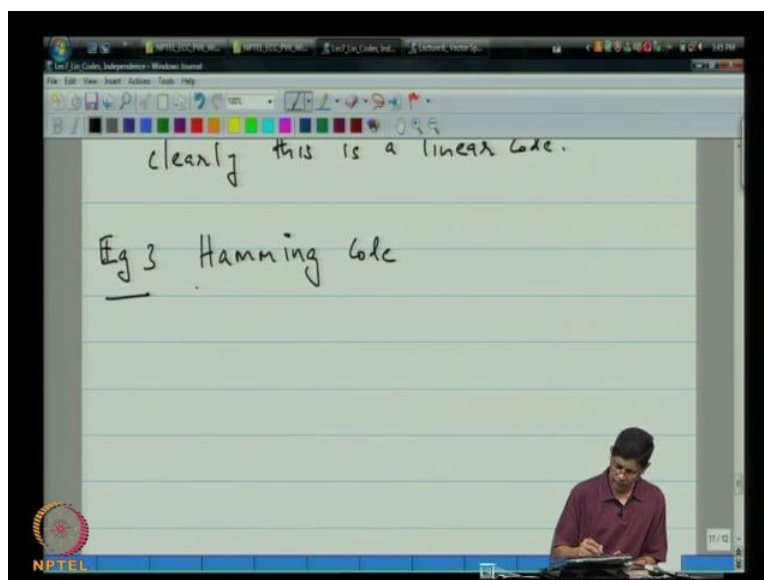
and a linear code is nothing but a subspace. So it follows from that that the single parity check code is a linear code.

(Refer Slide Time: 24:05)



Example 2: the repetition code. So here, the code is comprised of just two vectors and in order to check that it is a code you just have to check addition. Clearly the sum of the any two code words is a code word; therefore, it follows that this is also a linear code.

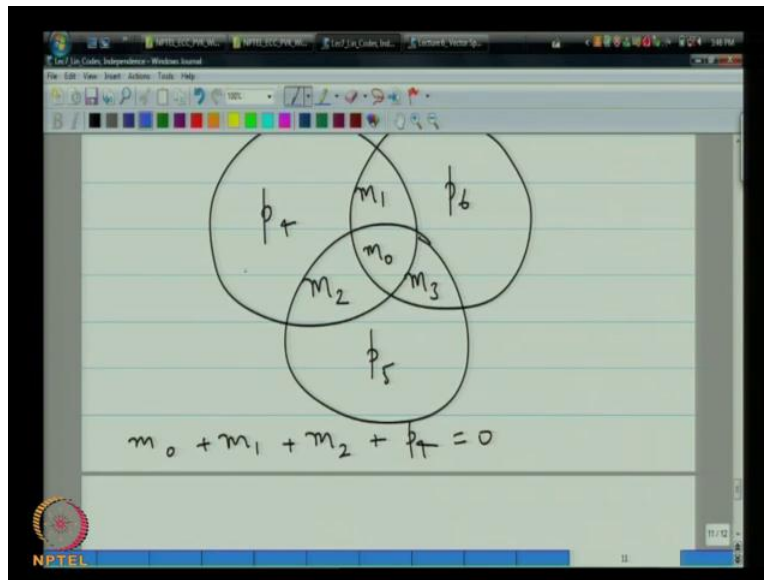
(Refer Time Slide: 24:58)





The more interesting question, so the two codes: the single parity check code, and the repetition code are both linear more interesting question is what about the hamming code?

(Refer Slide Time: 25:37)



So the Hamming code and I will draw the familiar picture again. So, the Hamming code if you will recall is a collection of binary bits arranged within three circle in such a way that, within each circle even parities actually satisfied. So, now for example: one of these parity equations would tell you that, it must be that  $m_0$  plus  $m_1$  plus  $m_2$  plus  $p_4$  is equal to 0. So, by looking at the parity condition in this circle you get this equation.

(Refer Slide Time: 26:51)

$$\begin{matrix}
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
 \begin{bmatrix}
 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
 1 & 1 & 0 & 1 & 0 & 0 & 1
 \end{bmatrix}
 & \begin{bmatrix}
 m_0 \\
 m_1 \\
 m_2 \\
 m_3 \\
 p_4 \\
 p_5 \\
 p_6
 \end{bmatrix}
 & = & \begin{bmatrix}
 0 \\
 0 \\
 0
 \end{bmatrix}
 \end{matrix}$$

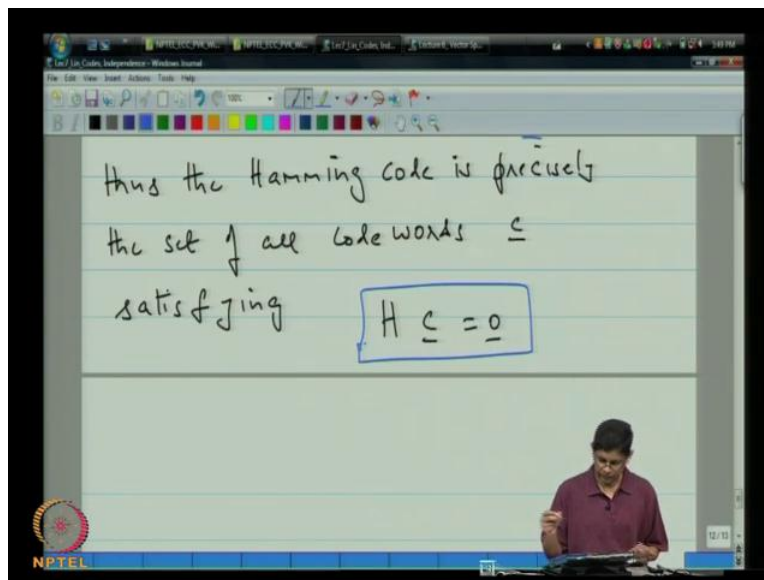
$H$ 
 $c$ 
 $0$

So, if you do that then you will see that, you can alternatively rewrite the equations in the following way. So, let me just write down in symbols as place holders for the coordinates. These are the 6 coordinates and we have in all 3 parity check equations.

So, the first one checks for 0 1 2 and 4. So, I will say 1 1 1 0 0 (Refer Slide Time: 25:37) the second one checks for 0 2 3 and 5, 0 2 3 and 5. The last one checks for 0 1 3 and 6. So these in a sense represent the parity checks. And now, if i just add a column vector and set this equal to 0 0 0 then it will be clear that there is an equivalence between the circle diagram and this matrix equation. So, I have  $m_0 m_1 m_2 m_3 p_4 p_5$  and  $p_6$ . So, let us call this matrix and label this as  $H$ . Now, this thing here is our code word and this is the 0 vector.

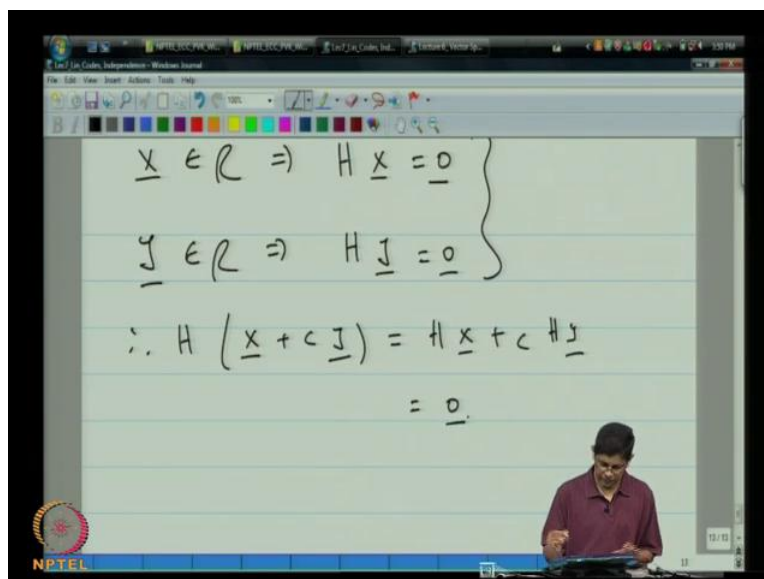
So, what we are saying is that, an alternative way of actually describing the Hamming code is simply to say that, it is the set of all vectors which satisfy an equation of the form  $h \cdot c$  equal to 0. Or, in other words the code is simply the set of all vectors which lie in the null space of  $H$ .

(Refer Slide Time: 29:36)



Thus, the Hamming code is precisely the set of all code words  $c$  satisfying  $H$  times  $c$  equal to 0. So, now we want to verify that, this in fact defines a linear code.

(Refer Slide Time: 30:27)



So let us, apply our test. Now,  $x$  in the code implies that  $H$  times  $x$  is equal to 0  $y$  in the code implies that  $H$  times  $y$  is equal to 0. So, it follows that therefore,  $H$  times  $x$  plus  $c$   $y$  is equal to  $H$  times  $x$  plus  $c$  times  $H$   $y$ . So this is 0.

(Refer Slide Time: 31:00)

The image shows a digital whiteboard with handwritten mathematical derivations. The text is as follows:

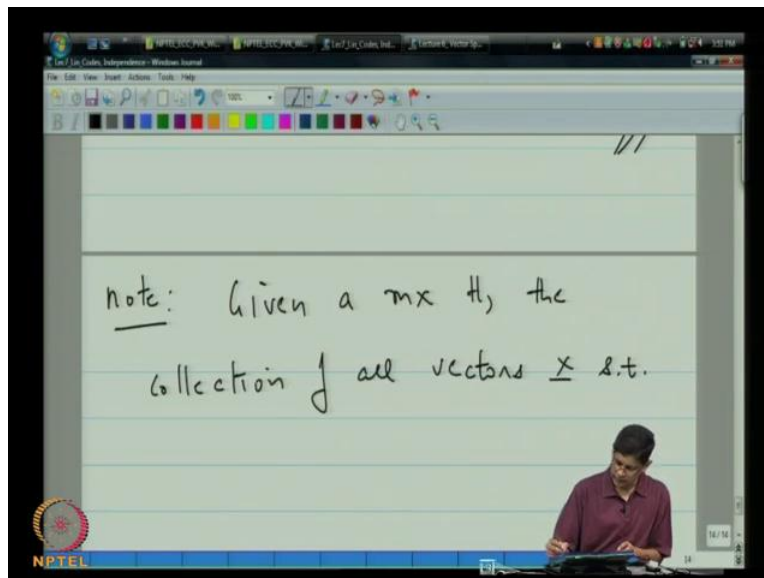
$$\underline{J} \in \mathcal{C} \Rightarrow H \underline{J} = \underline{0}$$
$$\therefore H (\underline{x} + c \underline{J}) = H \underline{x} + c H \underline{J}$$
$$= \underline{0}$$

$\therefore \{ \text{the Hamming code is a} \}$   
linear code.

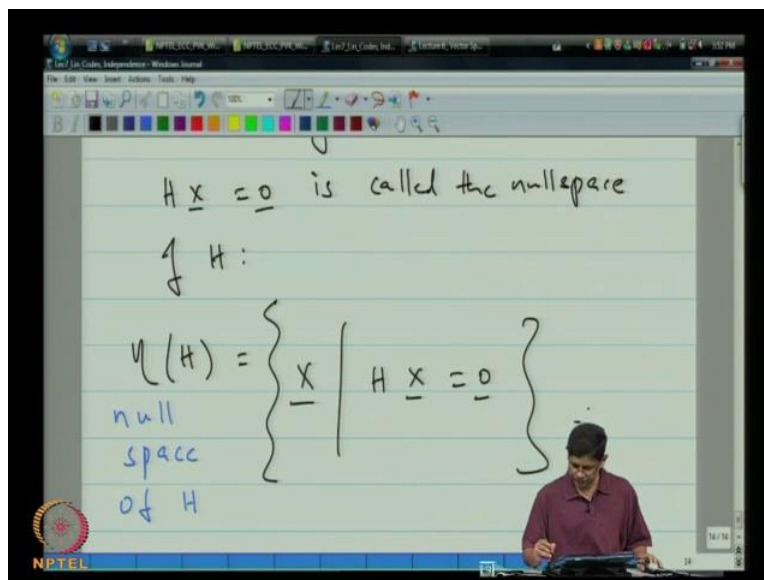
The whiteboard interface includes a toolbar with various drawing tools and a status bar at the bottom with the NPTEL logo and a slide number '13'.

Therefore, the Hamming code is linear. But you will notice just a quick remark here that in fact, what is actually true is that, any code which is defined through a matrix by saying that, here is the matrix  $H$  and the code is defined be the set of all vectors such that, that matrix times of vector is  $0$ . So now, the collection of all such vectors is called the null space of the matrix. And it follows from what we have just discussed is that, the null spaces always a subspace and therefore, defines a linear code.

(Refer Slide Time: 32:06)

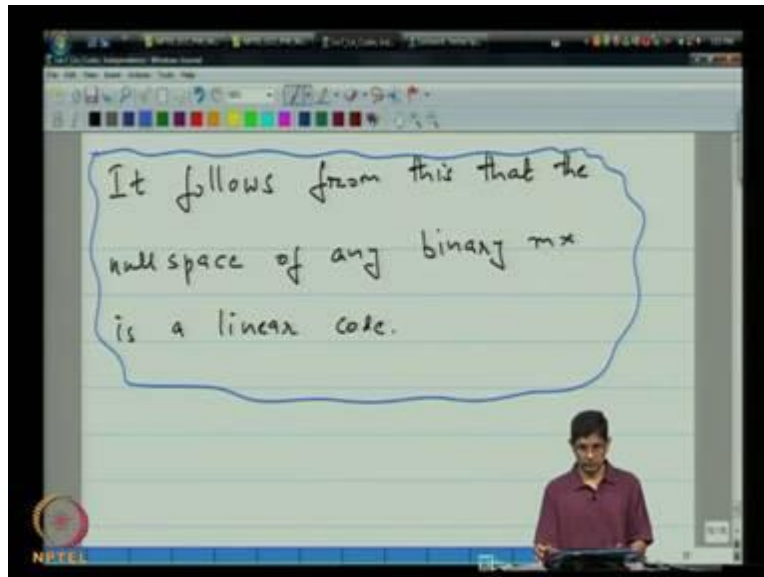


(Refer Slide Time: 32:32)



So, note: given a matrix  $H$  the collection of all vectors  $x$  such that  $H$  times  $x$  equal to  $0$  is called the null space of  $H$ . So, the null space is written, so this means null space of  $H$  is the set of all vectors  $H$  such that  $h x$  equals  $0$ . So, it follows from this. So, null spaces are terms that, you will frequently encounter in linear algebra, but also encoding theory.

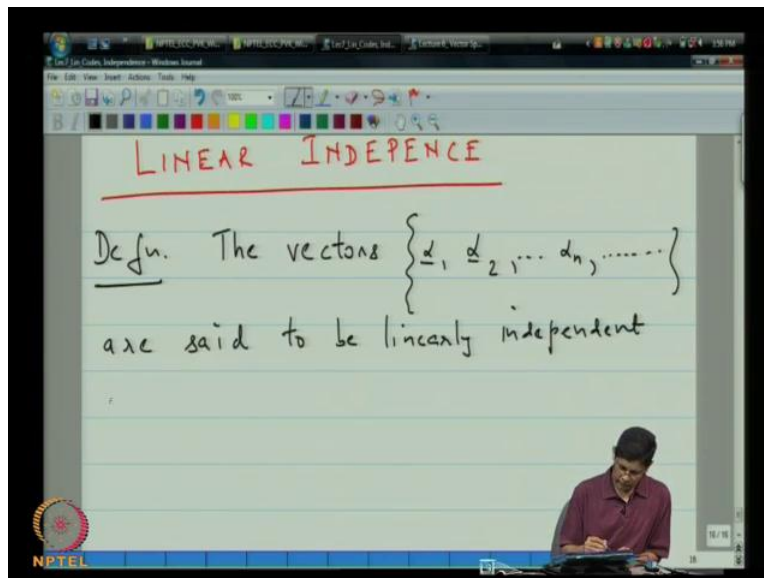
(Refer Slide Time: 33:32)



It follows from this that; the null space of any binary matrix is a linear code. Now, we will move on to another notion that is introduced in linear algebra and that is the notion of linear independence. So, we just have couple of items more to go relating to linear algebra and then we will be done with it and we will move on to dealing focus on error correcting codes. So, one is the notion of linear independence. What does it mean to say? Set of vectors is linear independent.

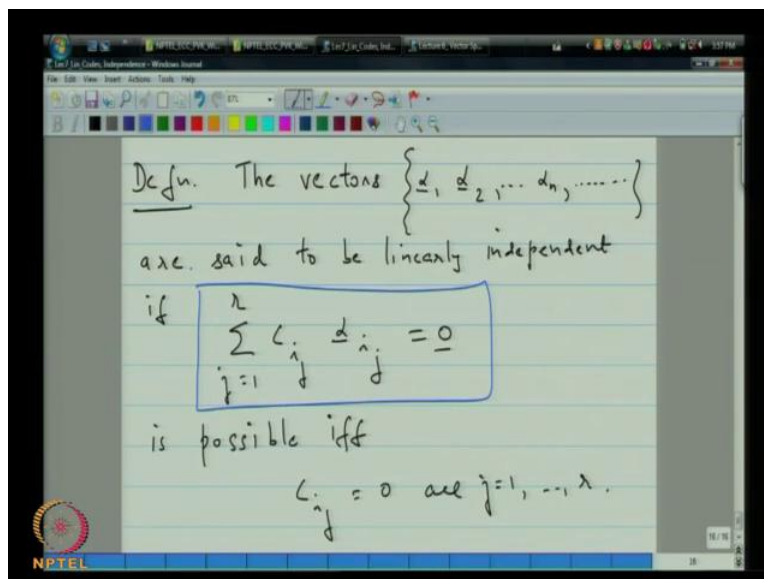
And after that we are going to talk about the notion of spanning what does it mean for a set of vectors to span a space and you may have an intuitive idea of it. But the aim here is to try to make that concrete and when you put, the notions of linear independence and spanning together then that takes you in the direction of defining something that is called a basis; A basis for a vector space. And amongst other uses the basis also is useful because it allows you to define the size of a vector space. In coding theory, it also useful in terms of allowing you to construct matrices that enables you to encode and decode the code as we will see later.

(Refer Slide Time: 35:53)



So let us, go on to the notion of linear independence. The vectors:  $\alpha_1, \alpha_2, \alpha_n, \dots$  dot dot dot. So, let me just make that clear here little bit clearer.

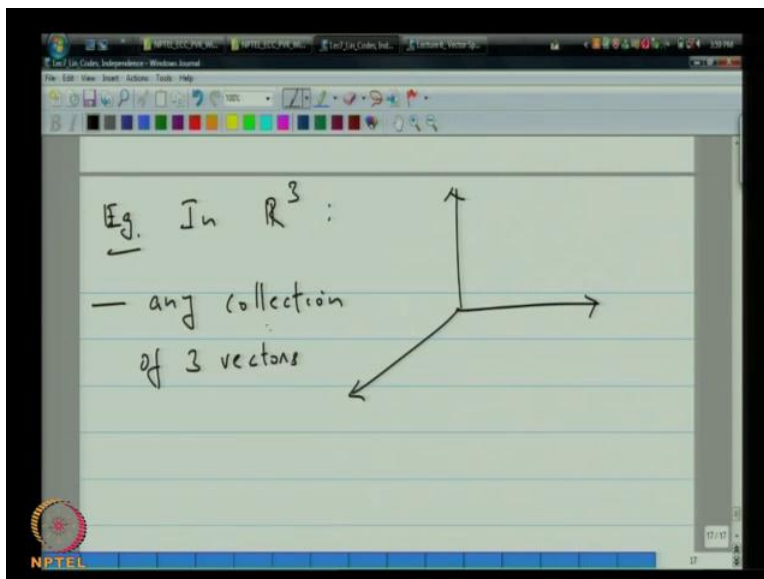
(Refer Slide Time: 37:14)



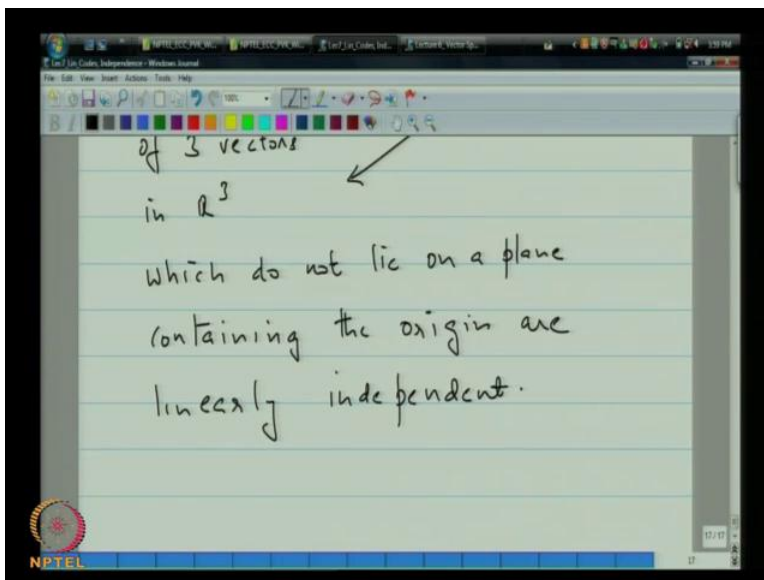
So, this could continue on up to infinity; are said to be linearly independent, if  $\sum_{j=1}^r C_j \alpha_j = 0$  is possible is possible if and only if  $C_j = 0$  for all  $j$  equals 1 to  $r$ . So, the test of linear independence is that, you are taking a linear combination of

vectors that is, you are scaling and adding you are taking a bunch of vectors you are scaling them individually and then you are adding, and if that sum 0 if and only if all those scaling coefficients are 0, then they are said to be linearly independent.

(Refer Slide Time: 38:45)



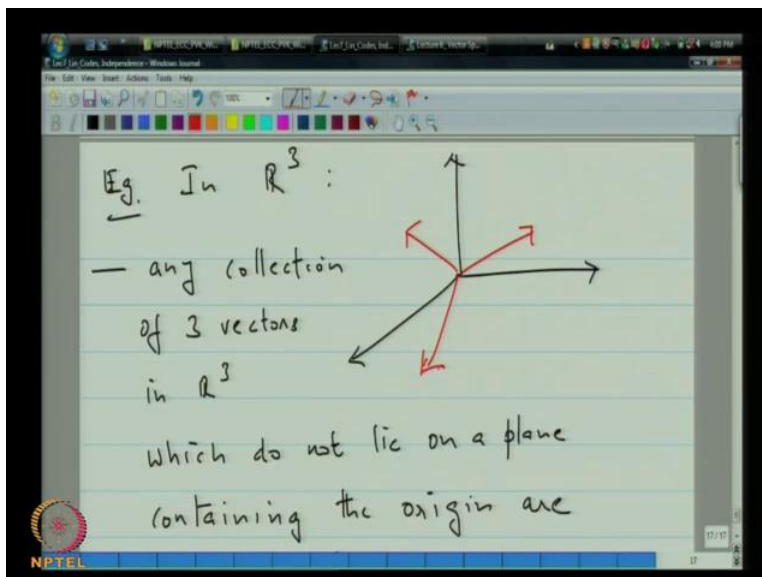
(Refer Slide Time: 39:30)





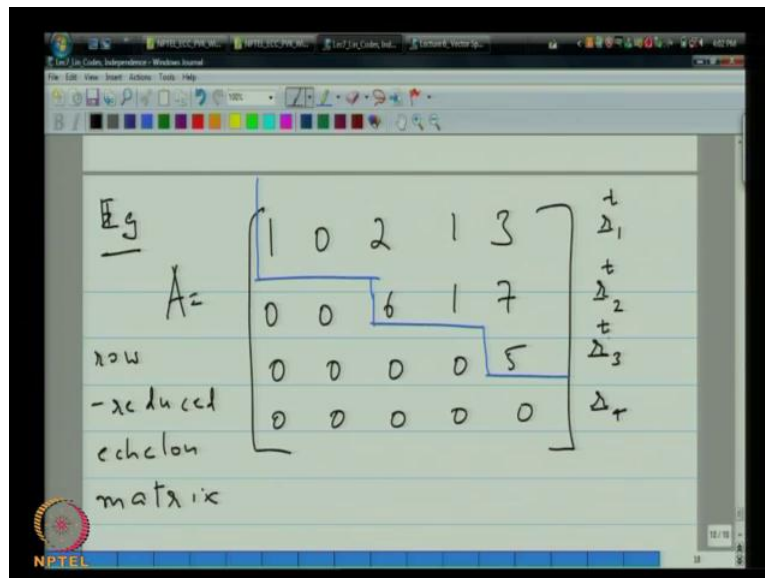
Now, what are some examples of linear independence? Example: in  $\mathbb{R}^3$ . So, if you are talking about three-dimensional space, then what is true is that any collection of 3 vectors in  $\mathbb{R}^3$  which do not lie on a plane containing the origin are linearly independent.

(Refer Slide Time: 40:26)



So, I might for example take, if I took 3 vectors like this if I took 3 vectors like this and if I could ensure that, there was no plane which contains plane through the origin which contains these three vectors then they are linearly independent. Now, I admit that, if you have not had linear algebra this may be a little bit quick for you. But the reason for including this is, that perhaps it is better to give some background rather than none at all. So, that is the spirit in which I am doing this.

(Refer Slide Time: 41:25)



Another example, of linear independence, supposing I take matrix of the form; so let us say we take a matrix of this form. Now, if you have taken linear algebra then you will realize that, this is what is known as row reduced Echelon matrix. Echelon simply means staircase form and by actually linking these non-zero entries they way I have actually shown it you can see that there is a staircase pattern that is actually formed. Now, with respect to this matrix; let say that, you are trying to actually prove that, the rows are either linearly independent or not.

Let us go back to the pad and supposing you try to take label these rows. So, let me call this row vector:  $r_1$ ,  $r_2$ ,  $r_3$  and  $r_4$  and I am going to put superscript  $t$  here on each of them, because by default, in our course, vectors will be column vectors.

Since these are row vector, I am going to put a transpose and if I were to ask the question are these linear independent? Then if you go back to the definition and the definition ask you to take to scale these vectors and add them, but it is just obvious just looking at the particular structure this matrix that only way in which you can take a linear combination of  $r_1$   $r_2$  and  $r_3$  is if those coefficients are zero. Now, just the note of caution, I am excluding  $r_4$  any collection of vectors, which contains zero vector is automatically independent set, because you can just scale that and get zero using a non-zero coefficient.

(Refer Slide Time: 43:53)

row

0	0	0	0	5
0	0	0	0	0

reduced echelon matrix

$\Delta_3$   
 $t$   
 $\Delta_r$

matrix

— {the nonzero rows are linearly independent}

So, the conclusion here is that the nonzero rows are linearly independent. Now, also one might be interested in the columns what can one say about the columns?

(Refer Slide Time: 44:25)

Eg:

$A =$

1	0	2	1	3
0	0	6	1	7
0	0	0	0	5
0	0	0	0	0

row

reduced echelon matrix

$t$   
 $\Delta_1$   
 $t$   
 $\Delta_2$   
 $t$   
 $\Delta_3$   
 $t$   
 $\Delta_r$

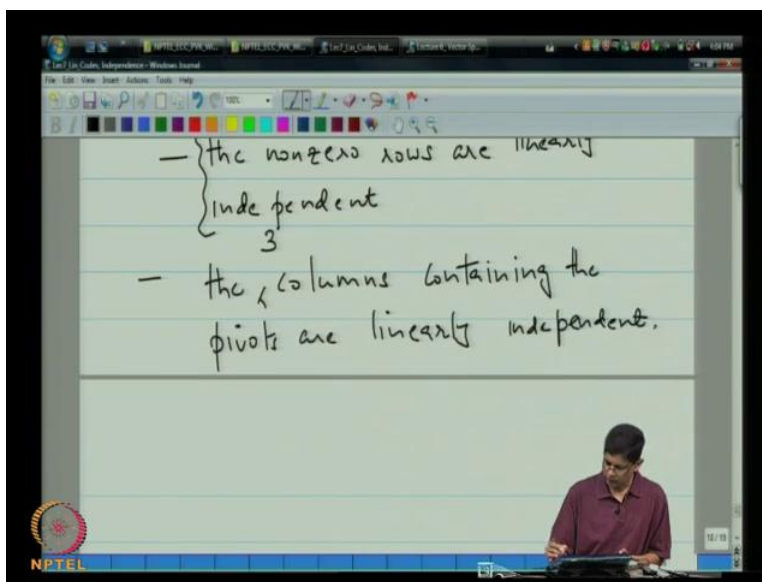
matrix

— {the nonzero rows are linearly independent}

So let us take a look at this, now again going back to linear algebra terms calls the first non zero entry each of the nonzero rows as they pivot. And by using similar arguments you can actually

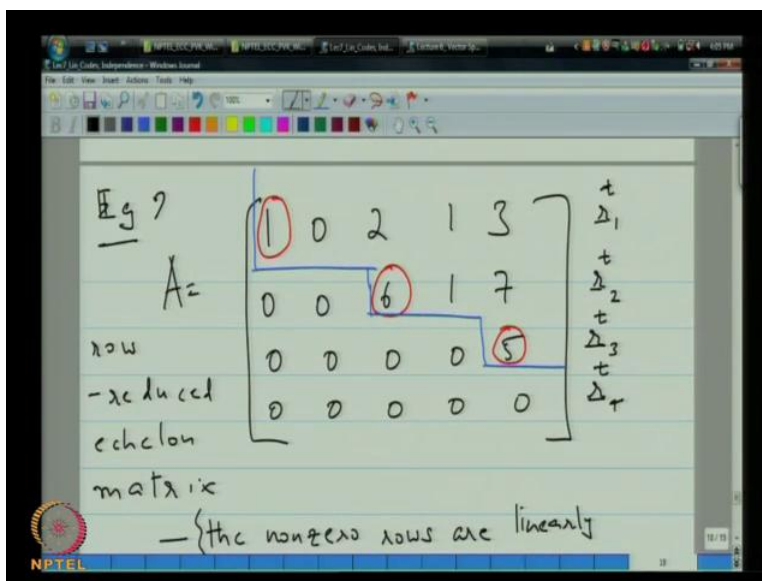
show that the columns containing the pivots are linear independent. So, in this case of particular matrix columns 1 3 and 5 are linearly independent.

(Refer Slide Time: 44:56)



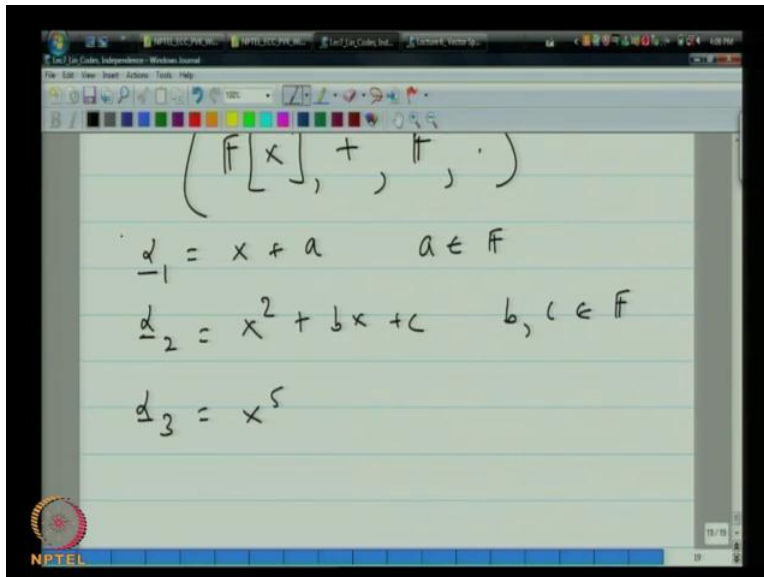
The columns containing that pivots are linearly independent. So, let me put down 3 are linearly independent, that is it for this example.

(Refer Slide Time: 45:36)



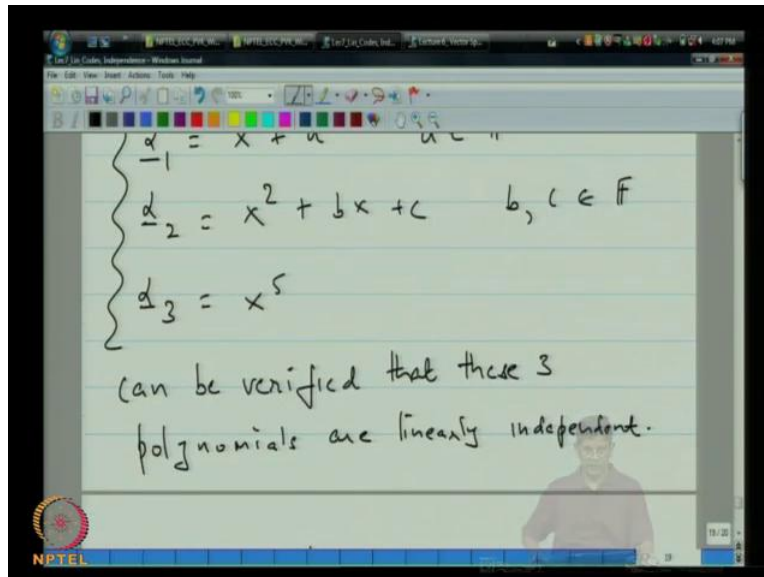
So this is example two.

(Refer Slide Time: 45:47)


$$(\mathbb{F}[x], +, \cdot)$$
$$\alpha_1 = x + a \quad a \in \mathbb{F}$$
$$\alpha_2 = x^2 + bx + c \quad b, c \in \mathbb{F}$$
$$\alpha_3 = x^5$$

Third example we will look another different structure, so example three and by way of this example I will introduce I will bring back the collection of polynomials that we encountered earlier. So, the setting for this example, is the vector space  $\mathbb{F}[x]$  plus  $\mathbb{F}$  dot. So, this is the setting and so examples of vectors might be  $\alpha_1$  is  $x$  plus  $a$ , where  $a$  belongs to the field or  $\alpha_2$  is  $x^2$  plus  $b$   $x$  plus  $c$  where  $b$  and  $c$  belong to  $\mathbb{F}$  and  $\alpha_3$  might be  $x^5$ .

(Refer Slide time: 47:20)

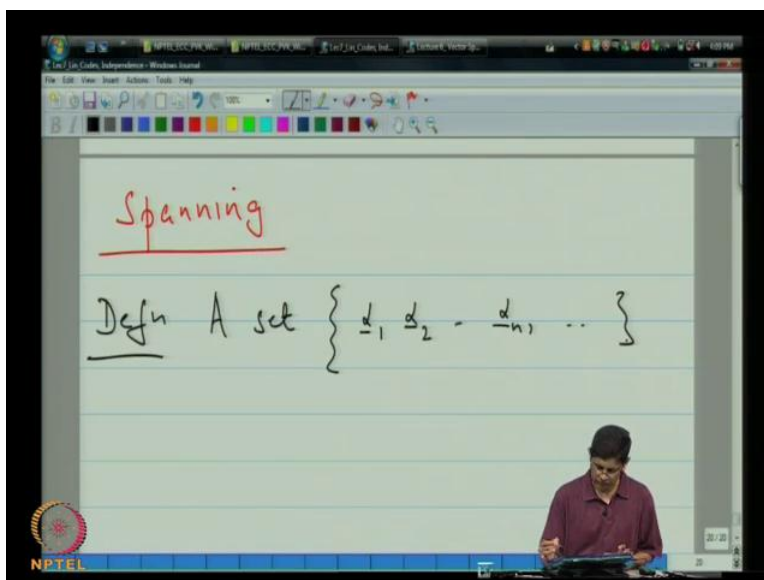


And again, you can actually satisfy yourself that these are linear independent there is no linear combination of them in which the three combining coefficients are nonzero can actually, give you zero can can be verified that these three polynomials are linearly independent.

Now, as you can see in our examples, we looked at three examples which were quite different in nature. In the first place we looked at three dimensional Euclidean space and we looked at vectors in three dimensional Euclidean space.

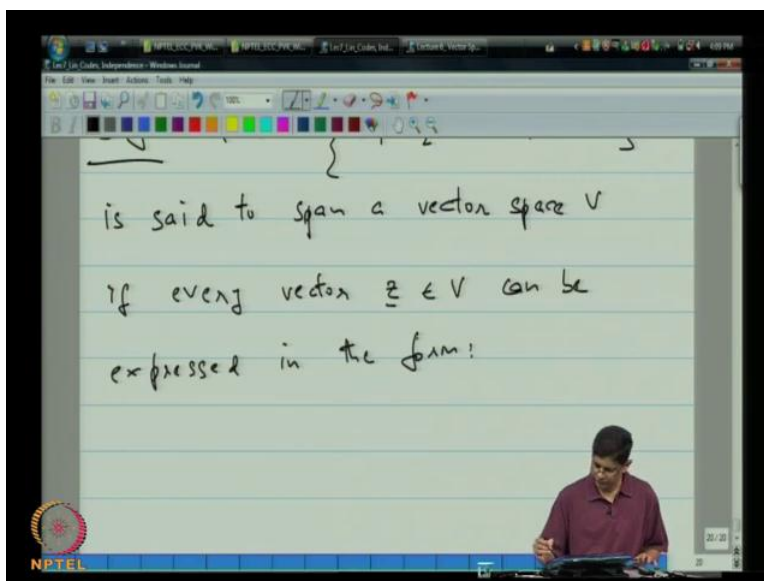
In the second example we will looking at the rows of a row reduced Echelon matrix where as the last example was related to polynomials. So, that the three examples of different in nature. The nice thing about actually working in an abstract frame work in the kind of frame that linear algebra provides it allows you to simultaneously address these different examples through a common definition and a common notion of independence.

(Refer Slide Time: 48:56)

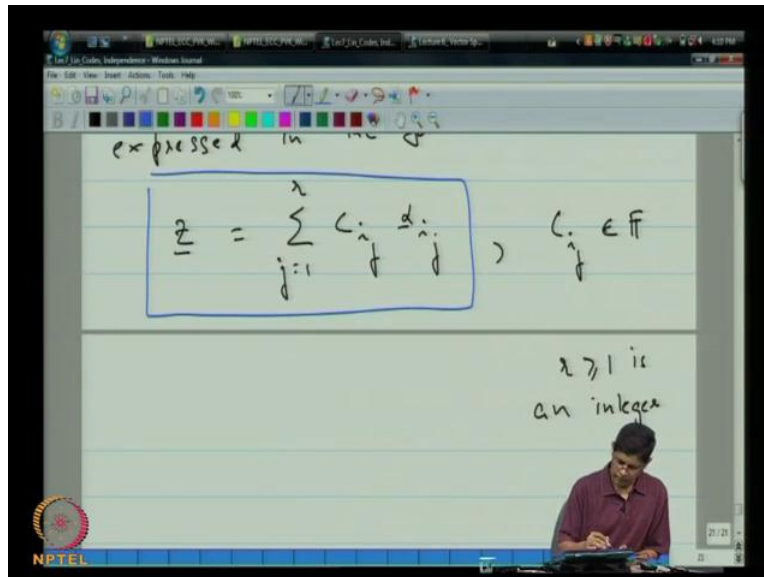


Now, what we will go on to is in another notion that of spanning again this comes from linear algebra. So, once again we will begin with a definition.

(Refer Slide Time: 49:35)

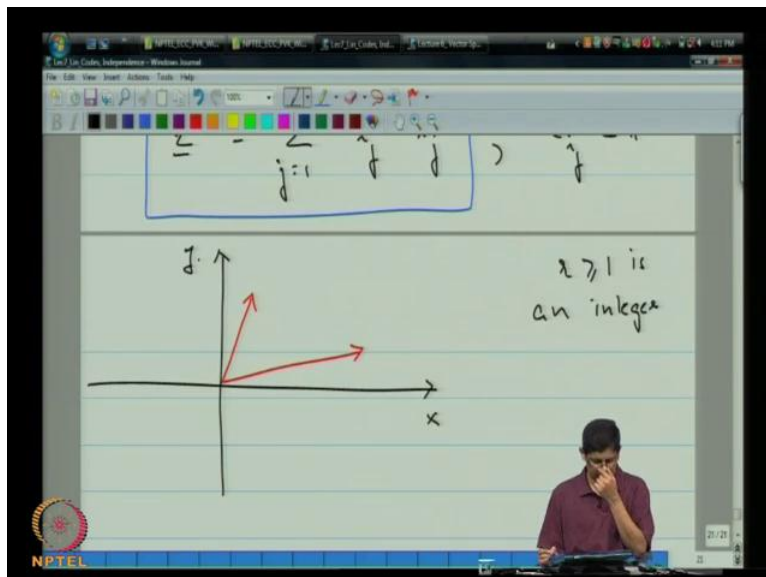


(Refer Slide Time: 50:22)



A set  $\alpha_1, \alpha_2, \dots, \alpha_n$  is said to span a vector space  $V$  if every vector  $Z$  in  $V$  can be expressed in the form  $Z = \sum_{j=1}^r c_j \alpha_j$  where the  $c_j$  come from the field and where  $r$  is some integer.

(Refer Slide Time: 51:17)

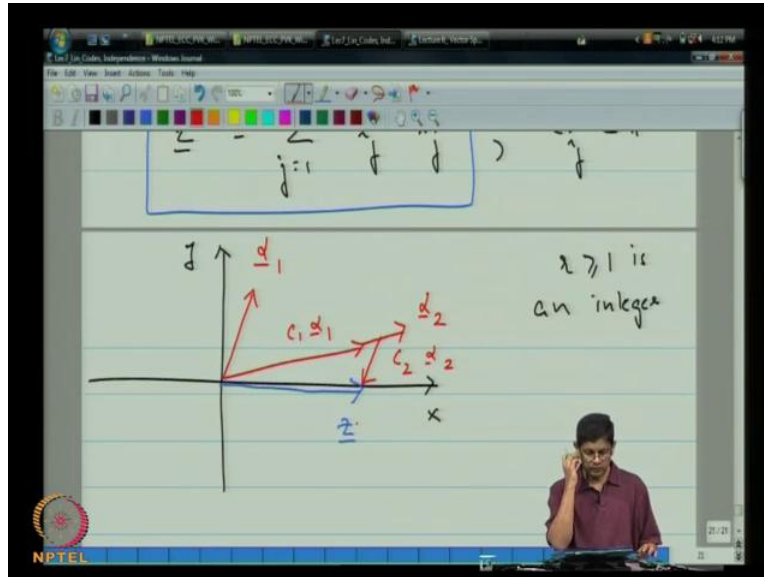


So, the notion of spanning is just that you should be able to derive from a certain basic set you should be able to derive other vectors. As the simple geometric example, one could perhaps



consider picture in two-dimensional space; supposing you took let us say a couple of vectors. One vector like this and let us say another vector like this. Then you can see that so this is you are x and y direction that every vector in the vector space can be derived as a linear combination of these vectors.

(Refer Slide time: 51:57)



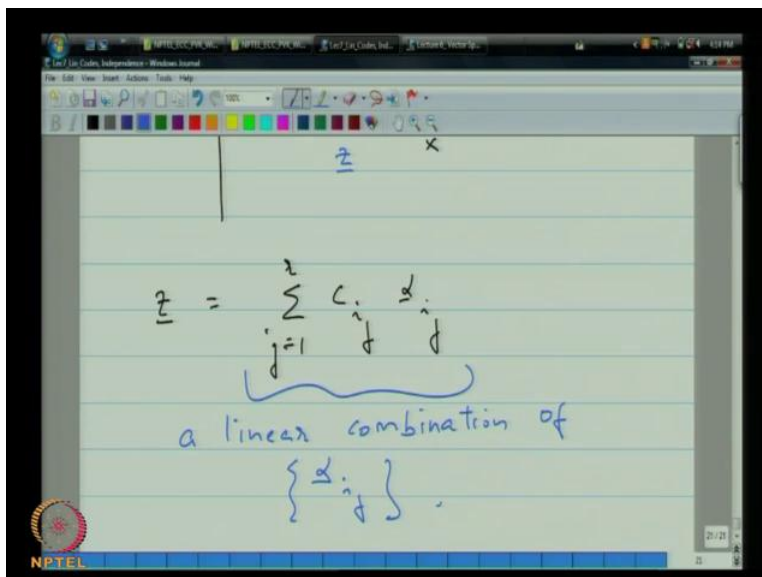
For example: supposing I wanted to derive let us say a vector along the x axis like this. Then what I could do is I could move, I could scale this to some point here. Then I could figure out a parallel line here. And you can see that by taking by scaling, so let us call these vectors alpha 1 and alpha 2 and let say that, this is your target vector Z.

So, let us say that alpha 1 was this. Let me do something here; let us move this over here, and so let us say that this vector here is  $c_1 \alpha_1$  is  $c_1 \alpha_1$  and this vector here was  $c_2 \alpha_2$ . So, that means by scaling the first vector and scaling the second adding you able to recover Z so this is what spanning means.

This  $c_2$  in this particular case would be negative, because you are going in the opposite direction. And the fact that these lines are parallel means that you are scaling the same vector. So, this is the idea of spanning that you can derive other vectors by starting out from these vectors.

Now, (Refer Slide Time: 48:56) we have defined what it means for a set to span a vector space. And by the way an expression of this form that you see over here an expression of this form is called a linear combination of the vectors  $\alpha_i$ .

(Refer Slide Time: 54:05)



$$\underline{z} = \sum_{j=1}^r c_j \alpha_j$$

a linear combination of  $\{\alpha_j\}$ .

I will just make a quick note of that and with that we learn the lecture. So,  $\underline{z}$  is equal to  $\sum_{j=1}^r \alpha_j c_j$  is equal to 1 to  $r$ . This example this is what we mean by a linear combination of the vectors  $\alpha_i$ .

So, to summarize what we did in today's lecture is we started out from test for a subspace, and I went through the test and I showed you why it works. We applied it to verify that in an example then I defined linear codes a subspaces, we could directly apply the test for sub spaces and verify and check that the 3 example we had encountered are actually linear codes.

Then we defined the notion of linear independence abstractly we looked at some examples and now we are examining the notion of spanning. So that is where we will pick up from, in the lecture, thank you.