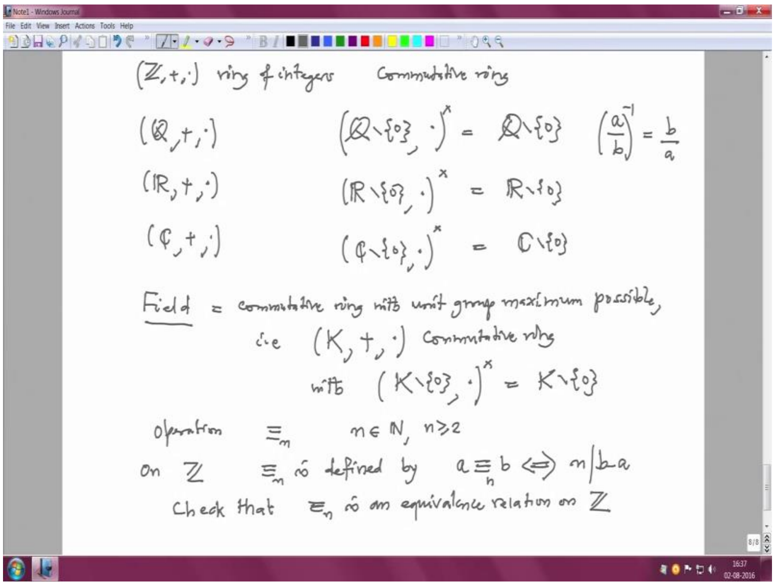
Linear Algebra
Prof. Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore

Lecture – 02
Definition of Vector Spaces

Welcome back to the second half of the first lecture. Remember we were considering the examples of fields. So far we have only seen the examples of the fields which were studied earlier, but now I want to consider another important example of a field, which is very important from the point of view of present applications.

(Refer Slide Time: 00:44)



$(\mathbb{Z},+,\cdot)$ ring of integers Commutative ring

$(\mathbb{Q},+,\cdot)$ $(\mathbb{Q}\setminus\{0\},\cdot)^{\times} = \mathbb{Q}\setminus\{0\}$ $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$

$(\mathbb{R},+,\cdot)$ $(\mathbb{R}\setminus\{0\},\cdot)^{\times} = \mathbb{R}\setminus\{0\}$

$(\mathbb{C},+,\cdot)$ $(\mathbb{C}\setminus\{0\},\cdot)^{\times} = \mathbb{C}\setminus\{0\}$

Field = commutative ring with unit group maximum possible, i.e $(K,+,\cdot)$ Commutative ring with $(K\setminus\{0\},\cdot)^{\times} = K\setminus\{0\}$

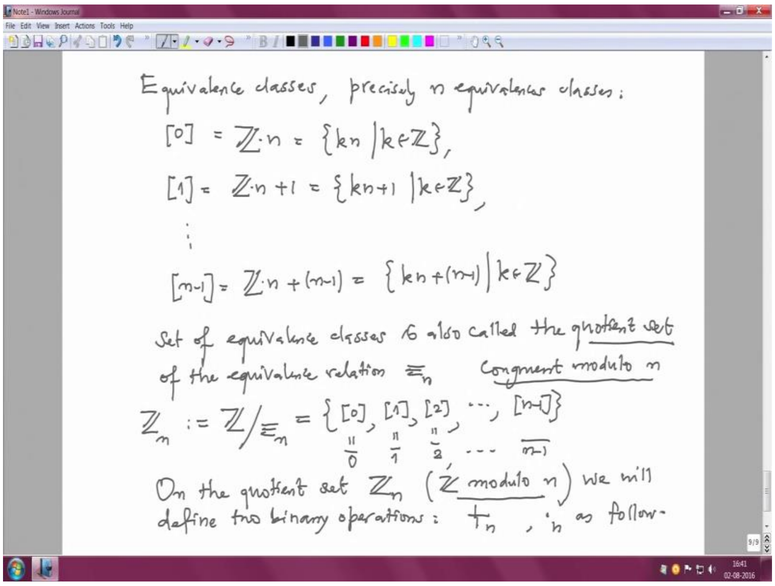
operation $\equiv_n$ $n \in \mathbb{N}$, $n \geq 2$

on $\mathbb{Z}$ $\equiv_n$ is defined by $a \equiv_n b \Longleftrightarrow n \mid b-a$

Check that $\equiv_n$ is an equivalence relation on $\mathbb{Z}$

So, first for this example, first let me recall in general the operation, congruence modulo N, where N is a natural number, positive natural number, and we will assume N is bigger equal to 2. So, this congruence modulo N is a relation on the set of integers, and Z is congruence modulo N is defined by a congruent to B mod N if and only if, N by it is B minus A, one checks is now, check that congruence modulo N is an equivalence relation on N. Now on integers, this means, what one need to check is this relation is reflexive symmetric and transitive.

(Refer Slide Time: 02:18)



Equivalence classes, precisely n equivalence classes:

$$[0] = \mathbb{Z}\cdot n = \{kn \mid k \in \mathbb{Z}\},$$

$$[1] = \mathbb{Z}\cdot n + 1 = \{kn+1 \mid k \in \mathbb{Z}\},$$

$$\vdots$$

$$[n-1] = \mathbb{Z}\cdot n + (n-1) = \{kn+(n-1) \mid k \in \mathbb{Z}\}$$

Set of equivalence classes is also called the <u>quotient set</u> of the equivalence relation $\equiv_n$ <u>Congruent modulo n</u>

$$\mathbb{Z}_n := \mathbb{Z}/\equiv_n = \{\underset{\overline{0}}{\overset{}{[0]}}, \underset{\overline{1}}{[1]}, \underset{\overline{2}}{[2]}, \cdots, \underset{\overline{n-1}}{[n-1]}\}$$

On the quotient set $\mathbb{Z}_n$ ($\mathbb{Z}$ <u>modulo n</u>) we will define two binary operations: $+_n$, $\cdot_n$ as follow.

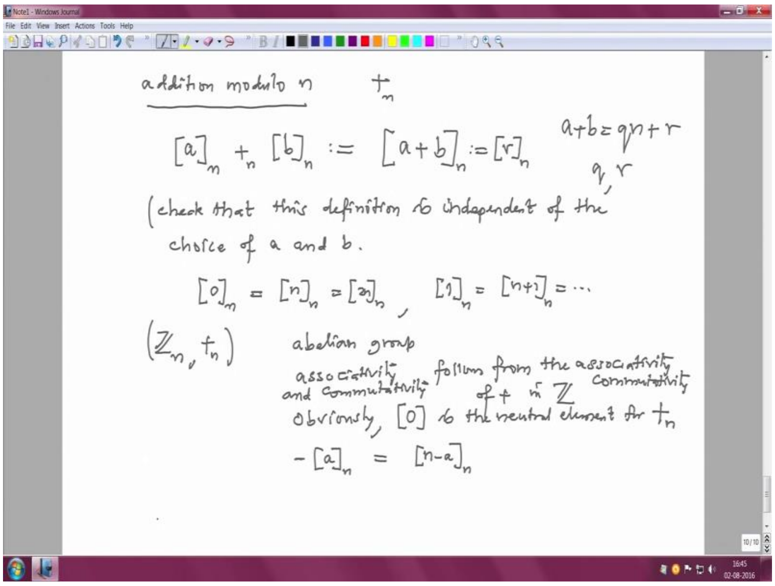
So, one can talk about equivalence classes. There are precisely in this case they are precisely N equivalence classes; namely equivalence class of 0, this is all integers which are multiples of N. So, I will as I said it is integer multiples of N K times N where K where is in integers, equivalence class of 1 is precisely by integers when you divide by N the reminder should be 1. So, one can denote them like Z times N plus 1, these are all integers of the form K N plus 1 where K where is in Z and so on.

So, equivalence class of N minus 1 is precisely the integers whose reminder after division by N is N minus 1. So, it is multiples of N plus N minus 1. So, this one call also the set of equivalence classes is also called the quotient set. The quotient set of the relation, of the equivalence relation. This is our case, it is congruent modulo. This is called congruent modulo N.

So, standard notation for that will give me Z divided by this relation. This is precisely the equivalence classes that is 0 1 2 and so on up to N minus 1. So, this is a set with exactly N element. So, this is also denoted by Z suffix N this is a standard notation I will use also. I will I will sometime use instead of this bracket, I will also use a notation 0 bar or 1 bar 2 bar etcetera, etcetera N minus 1 bar.

On these set, on the quotient set Z N Z mod N is I will keep calling Z modulo N. We will define 2 binary operations; one will be called addition modulo N, and the other is called multiplication modulo N as follows.

(Refer Slide Time: 06:21)



addition modulo n $\quad +_n$

$$[a]_n +_n [b]_n := [a+b]_n := [r]_n \qquad a+b = qn+r \quad q, r$$

(check that this definition is independent of the choice of a and b.

$$[0]_n = [n]_n = [2n]_n, \quad [1]_n = [n+1]_n = \cdots$$

$(\mathbb{Z}_n, +_n)$ abelian group

associativity and commutativity follows from the associativity commutativity of + in $\mathbb{Z}$

obviously, $[0]$ is the neutral element for $+_n$

$$-[a]_n = [n-a]_n$$

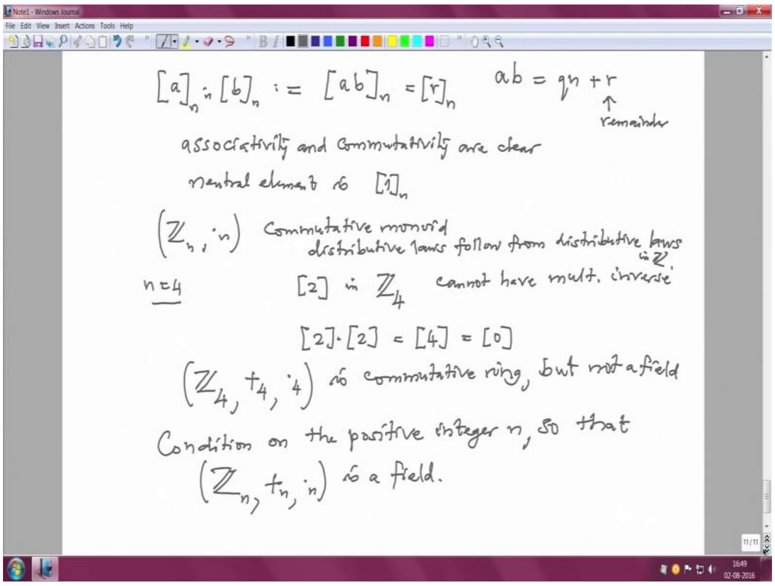
First the addition modulo N; that is sum suffix N. After sometime I will drop this suffix N in the notation when N is (Refer Time: 06:37) there is no chance for a confusion. So, if you take any A plus B. So, by definition you as add A and B as usual and take the residue. Residue means after dividing by N take the residue of a plus B; that means, A plus B write a plus B as Q times N plus R where Q is a quotient and R is a reminder then this is by definition the residue class of R.

So, now when I have to check that this definition check that this definition is independent of the choice of A and B for example, remember equivalence class of 0 or residue of 0 this 0 N is also same as N N or 2 N. And similarly, 1 is same as N plus1 N and so on. So, these definitions will need to check that this definition is independent of the choice of the integers A and B.

So, this will give us binary operation on the quotient set is Z mod N and now, the we will check that this is an Abelian group first of all associativity just follows on the associativity in the integers of plus in Z that we already are familiar with. So, that basically 0 is the neutral element for which operation plus N and we need to now check the inverse. So, if you have equivalence class A the inverse is; obviously, N minus A and minus of this is; obviously, N minus a because when you add them you get residue of this N which is 0.

So, that checks also commutativity associativity and commutativity follows on those of integers. So, we get an Abelian group.

(Refer Slide Time: 10:36)



$[a]_n \cdot_n [b]_n := [ab]_n = [r]_n$ $\quad ab = qn + \underset{\text{remainder}}{\underset{\uparrow}{r}}$

associativity and commutativity are clear

neutral element is $[1]_n$

$(\mathbb{Z}_n, \cdot_n)$ commutative monoid

distributive laws follow from distributive laws in $\mathbb{Z}$.

$\underline{n=4}$ $\quad [2]$ in $\mathbb{Z}_4$ cannot have mult. inverse

$[2]\cdot[2] = [4] = [0]$

$(\mathbb{Z}_4, +_4, \cdot_4)$ is commutative ring, but not a field

Condition on the positive integer n, so that $(\mathbb{Z}_n, +_n, \cdot_n)$ is a field.

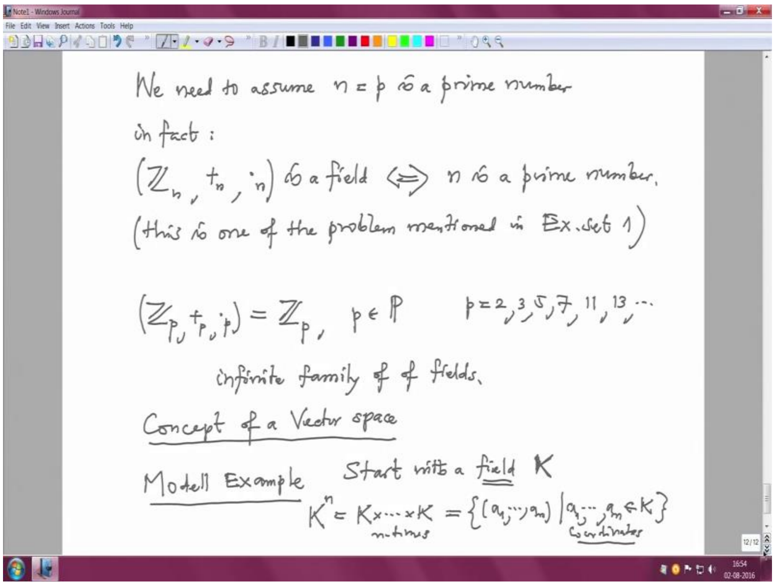
Now, the multiplication; so the definition of multiplication again we do the same way if you have equivalence class of a times equivalence class of B define multiple A and B as usual and take the residue class of A B. So, these mean again look at the integers A B divide these by N and look at the reminder this is a reminder. So, by definition this is the equivalence class of R.

Now, again associativity and commutativity are clear neutral element is the equivalence class of 1. So therefore, we get Z mod N these dot N dot N operation this is commutative monoid; obviously, for general N for example, if N is 4 the equivalence class of two in Z mod 4 cannot have multiplicative inverse, because 2 times 2 I will drop this N dot N I will just write dot this is by definition 4, but 4 is 0. So, this is 0.

So obviously, 2 cannot have multiplicative inverse, because if 2 have multiplicative inverse then I can multiple this equations by the inverse of 2 and then we can get 2 equal to 0 which is not possible. So, this Z mod 4 under the operation modulo 4 and multiplication modulo 4 this is commutatively but not a field, because for a field we need all non 0 element should have inverses I also forget to mention that you need to check here the distributive laws, but they follow from follow from distributive laws in Z.

So, one need to put a condition on the integer we started with the positive integer we started with. So, that Z mod N with this operations addition modulo N and multiplication modulo N is a field and these conditions are very easy to see.

(Refer Slide Time: 14:28)



We need to assume $n = p$ is a prime number

in fact:

$(\mathbb{Z}_n, +_n, \cdot_n)$ is a field $\Longleftrightarrow$ n is a prime number.

(this is one of the problem mentioned in Ex. set 1)

$(\mathbb{Z}_p, +_p, \cdot_p) = \mathbb{Z}_p$, $p \in \mathbb{P}$ $\quad p = 2, 3, 5, 7, 11, 13, \ldots$

infinite family of of fields.

Concept of a Vector space

Modell Example $\quad$ Start with a field K

$$K^n = \underbrace{K \times \cdots \times K}_{n\text{-times}} = \{(a_1, \ldots, a_n) \mid \underbrace{a_1, \ldots, a_n}_{\text{Coordinates}} \in K\}$$

We need we will need we need to assume N is a prime number P is a prime number. In fact, Z modulo N with respect to addition modulo N and multiplication modulo N is a field if and only if N is a prime number.

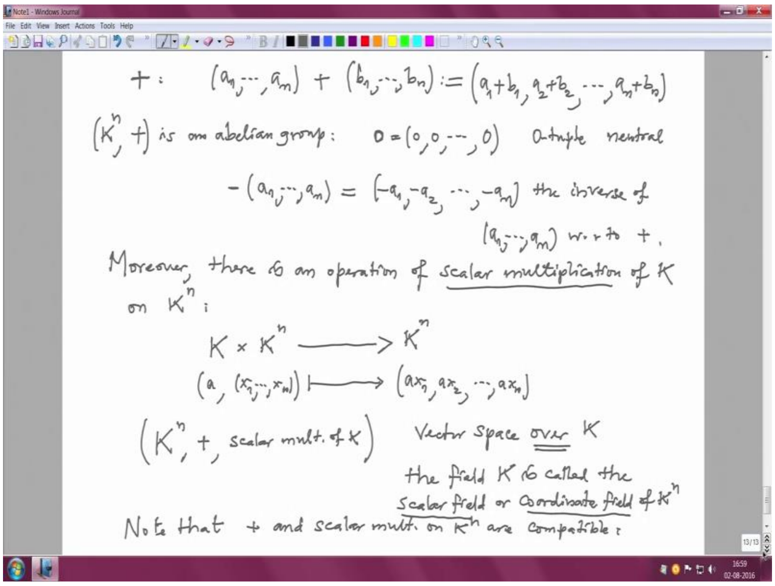
This is one of the assignments you will. So, this is one of the problems mentioned in one exercise set one by the way I will upload formal exercise sets as well as the supplements so that the supplements will contain more material which I have not spoken in this lectures. So, we have now new examples of a field only Z mod P plus P and dot P, but this every time I will not mention these operation explicitly and I will just write Z mod P it will be understood that there will be with the operation addition modulo P and multiplication modulo P and P varies in prime number for example, P is 2, 3, 5, 7, 11, 13, and so on.

So, we have an infinite family this is an infinite family of family of fields. So, we will you would also like to consider or vector spaces over these fields. So, now, I will come to the concept of a concept of a vector spaces as I mentioned in the introduction a vector spaces are generalized on the vectors we were studying and after sometime I will give more (Refer Time: 07:21) on this how and so on. Right now I want to consider one model example. So, model example.

So, start with the field K I will denote capital K field. So, I will not keep saying plus and dot it is now understood when I write field K is a field; that means, it had 2 binary operation plus and a dot with respect to plus it is an (Refer Time: 18:07) with respect to dot it is a monoid and all non 0 elements in this field are invertible with respect to multiplication and multiplication and addition. They are connected by distributive laws this is what we are given and now you consider K power N K power N is the Cartesian product of K N times K cross K K cross K N times.

This is by definition they are the tuples A 1 to A N where A 1 to A N are called coordinates of this tuple and they are elements of K. So, they are called coordinates a 1 is called first coordinate it is called second coordinate and so on these K power N. Obviously, addition there is a binary operation addition namely if I have two tuples a one to A N and B 1 to B N.

(Refer Slide Time: 19:16)



$+ :\quad (a_1, \cdots, a_n) + (b_1, \cdots, b_n) := (a_1+b_1, a_2+b_2, \cdots, a_n+b_n)$

$(K^n, +)$ is an abelian group: $0 = (0, 0, \cdots, 0)$ 0-tuple neutral

$-(a_1, \cdots, a_n) = (-a_1, -a_2, \cdots, -a_n)$ the inverse of $(a_1, \cdots, a_n)$ w.r.to $+$.

Moreover, there is an operation of <u>scalar multiplication</u> of K on K^n:

$$K \times K^n \longrightarrow K^n$$
$$(a, (x_1, \cdots, x_n)) \longmapsto (ax_1, ax_2, \cdots, ax_n)$$

$(K^n, +, \text{scalar mult. of } K)$ Vector Space $\underline{\underline{\text{over}}}$ K

the field K is called the <u>Scalar field</u> or <u>Coordinate field</u> of K^n

Note that + and scalar mult. on K^n are compatible:

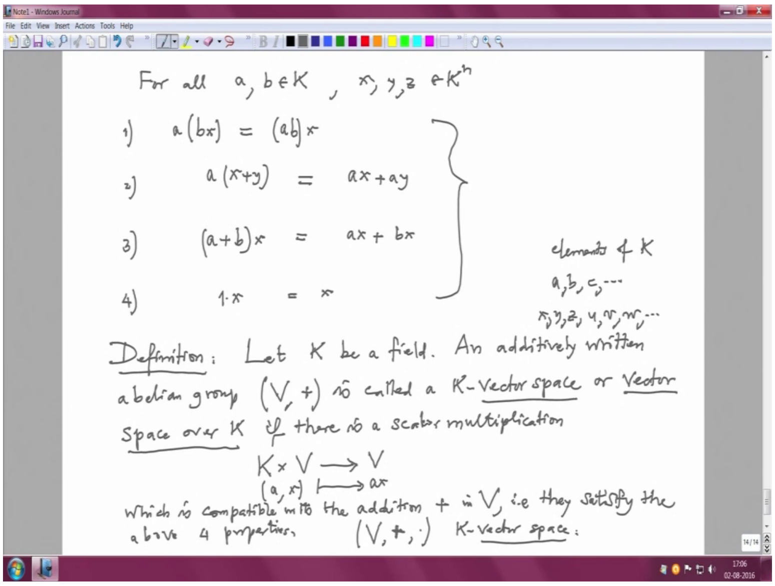
I will add them component wise; that means, I will define their additional these 2 tuples as I will add A 1 with B 1 in the field A 2 with B 2 and so on A N with B N.

Now, it is obvious that this plus with respect to plus this K power N, this is an Abelian group this is a Abelian group we got it from the Abelian group of the field K the action in the definition of addition in K to the definition of addition of tuples. So, for example, the neutral element is precisely the 0 this is 0 tuple this is this should be 0 0 0 all the this is called 0 tuple this is the neutral element in K power N inverse of A 1 to A N inverse of the tuple A 1 to A N which, because of the additive notation we should write minus and this is by definition it is minus A 1 minus A 2 and minus A N this is the inverse of A 1 to A N with respect to plus.

So, we got an Abelian group similarly, it has still more to go it has moreover there is a there is an operation of scalar multiplication of K on N on K power N which means we have a map from K cross K power N T O K power N mainly if I have any scalar a and a tuple X 1 to X N this is mapped on to just push the scalar inside. So, this is A X 1, A X 2 A X N where this coordinates. This multiple, this is inside there is a multiplication in K. So, we have used multiplication of K multiplication of the field K to define a scalar multiplication of K on these 10 tuples.

So, with this structure this K power N with this addition and a scalar multiplication of K this structure is called vector space over K this will K the field K is called the scalar field or coordinate field of K power N. So, this is our model examples with this model examples I will now, abstract I will make an abstract diffusion also I should mention here that one more point to mention here, that this scalar multiplication and the plus they are compatible with each other. So, you should mention note that plus and scalar multiplication on K power N are compatible; that means, it satisfy the following properties namely for all scalar I will keep calling elements of the fields as scalars and X Y Z as tuples.

(Refer Slide Time: 24:18)



For all $a, b \in K$, $x, y, z \in K^n$

1) $a(bx) = (ab)x$

2) $a(x+y) = ax + ay$

3) $(a+b)x = ax + bx$

4) $1 \cdot x = x$

elements of K

$a, b, c, \dots$

$x, y, z, u, v, w, \dots$

Definition: Let K be a field. An additively written abelian group $(V, +)$ is called a K-Vector space or Vector space over K if there is a scalar multiplication

$$K \times V \longrightarrow V$$
$$(a, x) \longmapsto ax$$

which is compatible with the addition + in V, i.e they satisfy the above 4 properties, $(V, +, \cdot)$ K-Vector space.

So, A B first whether I multiple A scalar B first I multiple the tuple X by B and then you get A an element in K power N then multiple by A, on the other hand I can multiple the two elements A and B in the field A B and then multiple X by this scalar. So, the result should be same. So, this is a property 1 property 2, if I add 2 tuples and multiple by scalar on the other hand I multiple X by scalar A and Y by scalar A and add the 2 tuples the result should be same so; that means, whether you add first and multiple by scalar or multiple by scalar and add these 2 operations are same.

Third one if I add 2 scalars in the field and multiple take the scalar multiplication of this mean scalar on X or you multiple scalar multiple X by scalar A multiple B by scalar X and add the 2 tuples this is a should be same forth. If I take multiplicative identity in K which we are denoting by 1 1 times X should be X. So, this is 1 time X is scalar multiplication on 1 of X or this is X this is these properties are very important and also very natural, because different people might calculate a formulas by simplifying in a different ways and these this properties ensure that two people calculating in a different way the answer will be same and they will compatible with each other.

So, that this is a reason that we demand this property. Now the general definition; so definition let K be a field to define a vector space, but we need a field first that is called a field of scalar field and additively written Abelian group that is V plus remember that I will now considering a new additive Abelian group V plus and we have also plus on the field K, but these two operations are different and they should the formulas we will should be clear from the context to where we are adding in a vector space or in a field and there should not be a confusion in this it should be clear from the notation we use as you normally I would like to use elements of K as A B C etcetera called scalars and elements of this Abelian group I will call X Y Z or U V W etcetera and these elements are called vectors.

So, it is additively written Abelian group V plus is called K vector space or vector space over K. If there is a scalar multiplication A scale you remember scalar multiplication in a map from K cross V to K or V to V is also I remember usually A in the pair a comma X the image of this under this scalar multiplication in simply A X which is compatible with the addition plus in V that is we satisfy the above 4 property.

So, vector space as remember V as 2 structures V there is A addition with respect to addition, it is an Abelian group and there is a scalar multiplication that I will just show it nothing or just dot. So, this is A K vector space. So, remember same set we or same Abelian group can be vector space in a different way depending on the scalar multiplication or the same set V with a different addition can become a different vector space.

So, we will continue this in the next lecture thank you very much for today. We will continue with our A theory of vector spaces in the next time.