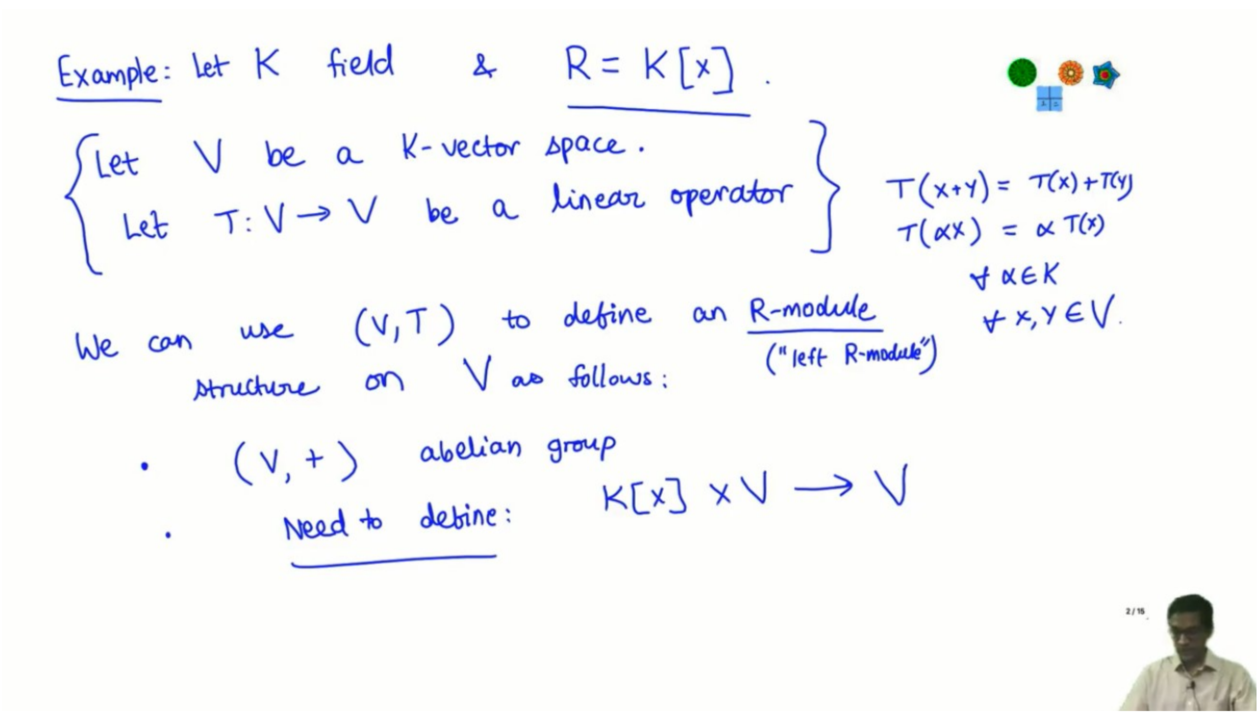
Algebra - I
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

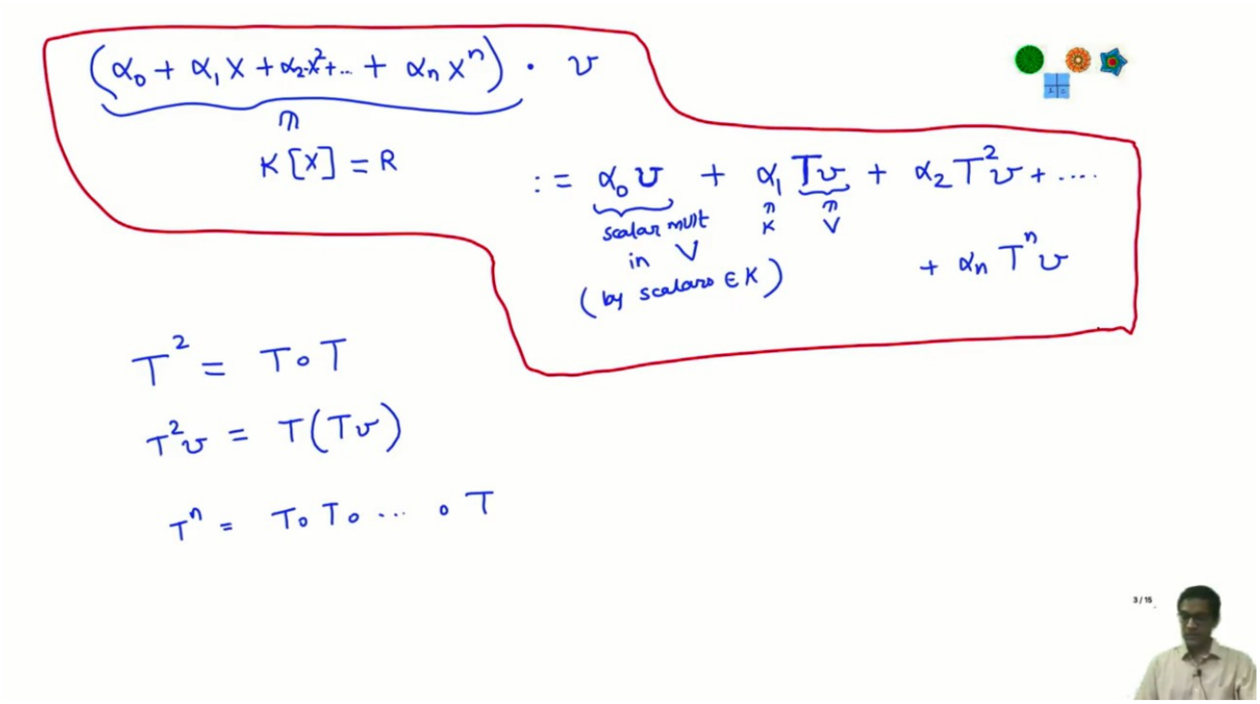
1. Lecture 52 [Modules over polynomial ring $K[X]$]

Let us look at modules over polynomial rings. We have already looked at one example of Modules over the ring of integers, there we showed it is just nothing, but the set of abelian groups those are exactly the modules. Now, let us look at polynomial rings now. So, what is a polynomial ring, what do we have in mind?

So, example so, let us take a field K and so, let K be a field and the ring that we will consider is the ring of polynomials in 1 variable x with coefficients in the field K ok. So, of course, you have you have seen this ring before looked at various properties of it ideals and so on and so forth. Now, let us try and understand what modules over this ring will look like? Ok. So, let me give you examples of modules first. So, let K sorry let V be a K vector space. So, let it be a vector space over the field K . So, it is a first piece of data I will start with and I also need another piece of information, which is a linear transformation on V ok.

Let T :V$\rightarrow$ V be a linear operator or a linear transformation ok, recall linear operator from linear algebra is just a map from $V \rightarrow V$, which satisfies a following properties, if I take $T(x+y) = T(x) + T(y)$. And, if I multiple if I sort of scalar multiple, then $T(\alpha x) = \alpha T(x)$





ok. And, this is now of course, for all α coming from the field K; for all xs and y is coming from the vector space V ok. So, this is the linear operator. Now, if I take a vector space and a linear operator on that vector space, this data here can be used to define a module over the ring R ok. How is that?

So, let us let us let me describe this construction, we can use this pair of information (V, T) to define an R modules structure on well on the same space V in fact ok. I can make V into an R module or a left R module as follows. So, when I say R module usually without without qualifying it I usually always mean left R module ok. So, when I say this I always mean left R module. And, note we have already said that left and right coincide if the ring is commutative which in this case is is it is in fact commutative here ok. We can use this to define an R module structure on V. So, let me describe the R-module structure as follows ok. So, what do we need to define an R module structure? well recall V is already an abelian group. So, there is nothing further to do there, I already have an addition on V what I need to define is really the scalar multiplication right.

So, I need to tell you, need to define the scalar multiplication map $K[X] \times V \to V$, which satisfies those 4 axioms ok. So, let us define it as follows, what are elements of $K[X]$ first? So, I need to tell you what a typical element of $K[X]$ looks like. So, let me let me take an element of $K[X]$. So, what is a element of $K[X]$? It is a polynomial . So, here is a typical element of $K[X]$. So, I need to define scalar multiplication by elements of the ring R ok.

Now, the scalars are not just elements of the field K alone, the scalars are actually polynomials in the variable x ok. So, this guy $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_n x^n$ is now a scalar really, because I am allowing scalars to come from my ring R ok. So, I should take this scalar and I should take some vector . So, ok let me not use X for vectors anymore.

So, may be even the the previous going back here, since I already have an X there. So, may be it is safer to you know call this variable X as something else. So, that there is no confusion with the other X. So, let me just say, let us use v_1 and v_2 here for my vectors. So, let me say $T\ (v_1 + v_2) = Tv_1 + Tv_2$,$T\ (\alpha v) = \alpha T(v)$ ok. And, this is for all v, v_1, v_2 in my vector space V ok, that was just the the definition of the linear transformation.

So, now, I I let me come back to my main object, which is to try and define a scalar multiplication. So, take this polynomial which is a element of my ring R. I should tell you how to scalar multiple it with a vector V right. Now, the definition as is as follows we we just try to do the most most intuitive thing. So, let us define it as .

So, let let let me look at the constant term α_0 is a constant term of the polynomial the constant term remember is an element of K ok, all the coefficients in fact are elements of K. So, I will take this this element α_0 of K and after all V is a K vector space right. I already know how to do scalar multiplication there; so, V is a vector in my vector space α_0 is a scalar from K. So, I already know how to multiple elements of K with elements of v.

So, this is $\alpha_0 v$ just the usual scalar multiplication in my vector space V, multiplication by scalars coming from K by scalars in K. So, this is already given right, I know that V I I started with a K vector space V. So, it is a $\alpha_0 v$ is just usual scalar multiplication of v with α_0 . Now, the trouble comes in the next term I have $\alpha_1 x$ right. Now, I need to somehow figure out a way of defining how this element acts on V. Now, if I have just $\alpha_1$of course, $\alpha_1 v$ is just the usual scalar multiplication, but I do not know what to do with the x here ok. So, that is really what this additional linear operator T is useful for. So, here is our definition. The second term $\alpha_1 x$, we make it act on v as follows x sort of acts like the operator T ok.

$T(v)$ now is again some vector in V, $\alpha_1$is the scalar in K . So, scalar in K times vector in V, I know how to do it because that is the scalar multiplication in the vector space (V,+) let us look at the next term x^2 right. This is now going to look like $\alpha_2 x^2$. So, I will define it as as follows this is just T^2 acting on V ok. Now, what is T^2? So, recall T^2 is just short hand notation for T composed with T. In other words $T^2 v$ is just the vector T acting on Tv , $+.... + \alpha_n T^n v$, again T^n just means a repeated composition of T n times ok.

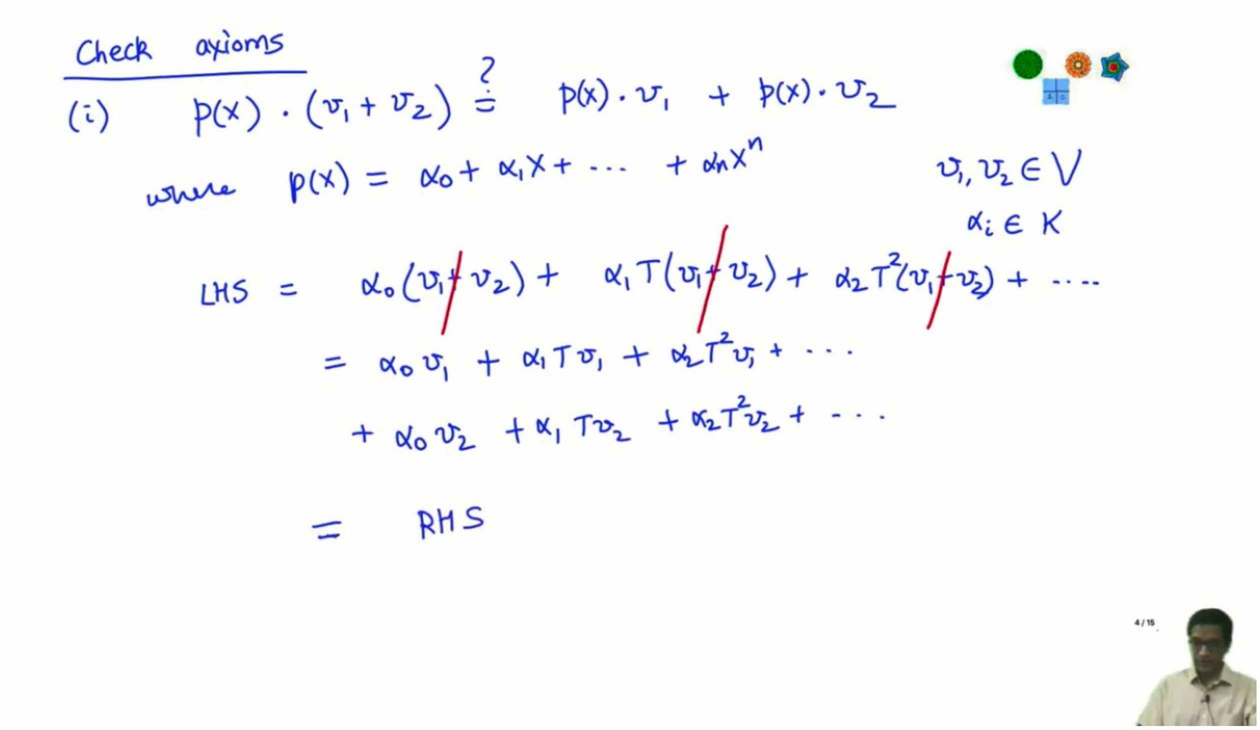
So, this is my definition, I make my definition in this manner. So, I say that my scalar this polynomial $(\alpha_0 + \alpha_1 x + ...) \cdot v$, gives me this answer $\alpha_0 v + \alpha_1 Tv + \alpha_2 T^2 v + ...$ and so on ok. Now, we have to check that this satisfies all the axioms ok. Once, we check that then of course, it is a well defined module. So, let us check the axioms. So, that is our task.

So, let us check the axioms ok. So, what is the first axiom say it says that, if I take a scalar so, in my case my scalar some polynomial in x. So, I will just call it $p(\ x)\ \cdot(v_1 + v_2)$ that should give me this polynomial acting on $p(x)v_1 + p(x)v_2$ ok, where so, have $p(x)$ I am just using as .

So, this is my polynomial $\alpha_0 + \alpha_1 x + ... + \alpha_n x^n$ And, of course, all the elements come from the appropriate spaces v_1 and v_2 come from V the alphas are all element of K ok. So, I have to check if this is true. So, is this true is a question right, according to my definition. Just a question of of writing out both sides so, observe that so, the formula that I that I wrote out. So, what is the left hand side? Therefore, this is just going to be α_0+ ok. So, let me write it as this $\alpha_0(v_1 + v_2) + \alpha_1 T(v_1 + v_2) + \alpha_2 T^2(v_1 + v_2) + ...$ and so on ok till they reach the nth term.

But, the key observation here is that each of these terms as actually splits into two pieces ok. So, $T\ (v_1 + v_2)$ remember T was a linear operator. So, I can write it as $Tv_1 + Tv_2$. If, T is a linear operator, T composition T is also a linear operator.

So, T^2 is linear. So, $T^2(v_1 + v_2)$ will again split into two pieces. So, α_0 multiplied by $v_1 + v_2$ is $\alpha_0 v_1 + \alpha_0 v_2$, because you have distributivity in the vector space V. So, I I sort of split this



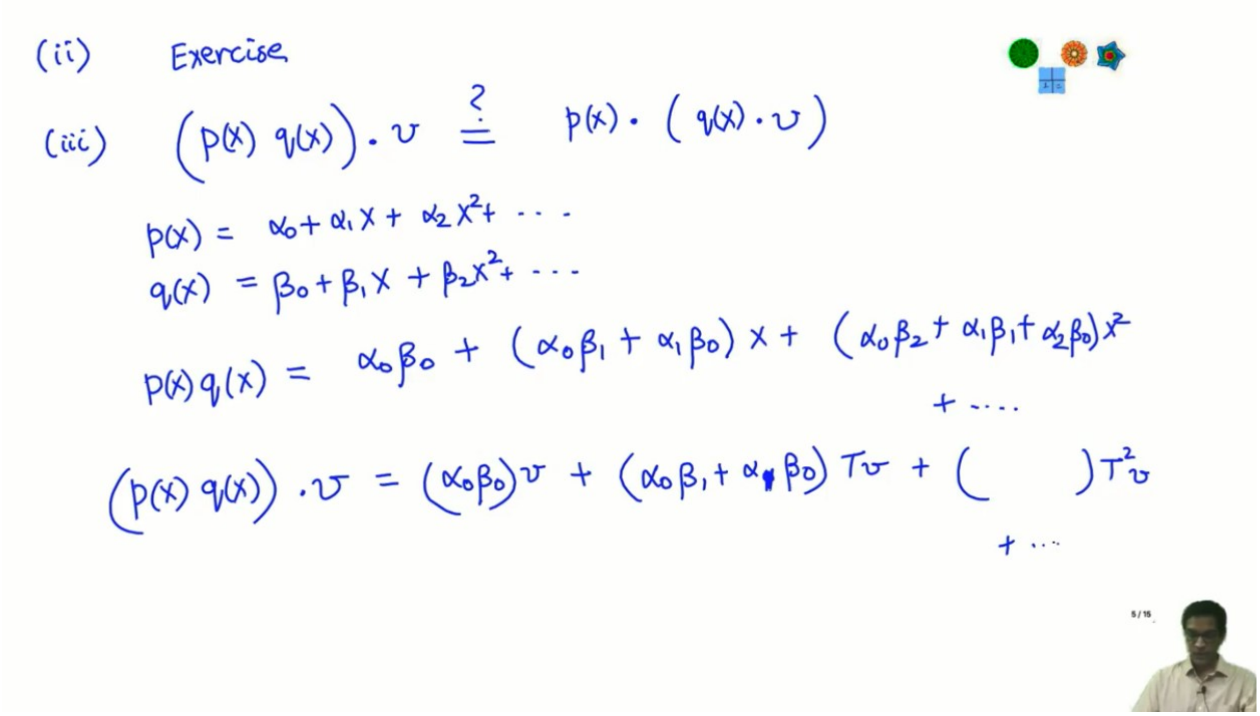
into two pieces I just write all the v_1's first $\alpha_0 v_1 + \alpha_1 T v1 + \alpha_2 T^2 v_1 + ...$ etcetera etcetera. And, then below it I write all the v_2 terms $\alpha_0 v_2 + \alpha_1 T v_2 + \alpha_2 T^2 v_2 + ...$ and so on. And, observe that is exactly the right hand side, where you have to sort of do it in two separate steps ok.

So, that is the the first axiom now now the second axiom is sort of similar it is in fact even easier, the second axiom just uses the fact that this is linear. So, I will just leave the second axiom for you to check it is an exercise. The third axiom which is that if I multiple two scalars ok. In other words I take two polynomials $p(x)$ and $q(x)$ and I multiple them in my ring R and then act on a vector V .

Then, the answer should be the same as the answer I get when I first take $p(x)$ acted on the answer that I get when I act $q(x)$ on v ok. So, this is what I need to check again. I need to see if this this statement is true for my third axiom and again let us write both sides out. So, what is p into q? So, now, this involves multiplication in my ring of polynomial. So, remember $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + ...$ blah blah blah till till some finite point $q(x)$ looks like $\beta_0 + \beta_1 x + \beta_2 x^2 + ...$ and so on.

Now, their product $p(x)$ times $q(x)$ is computed as follows right. So, what is a constant term it is $\alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)x + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)x^2 + ...$ and so on right. So, this is how we compute the product of of p and q. And, so, now, when we act the product $(p \cdot q)v$, what is it give us? Well we just have to do the following wherever you see, so, each of these numbers.

So, I write $(\alpha_0\beta_0)v + (\alpha_0\beta_1 + \alpha_1\beta_0)Tv + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)T^2 v + ...$ So, remember this term x means I should replace it with Tv, next term with $T^2 v$ and so on . So, that is my, that is how $p(x)q(x)$ acts. Now, let us compute the right hand side which is $p(x)$ acting on $q(x)$ acting on v. So, what is that mean I first have to figure out what $q(x)$ acting on v is



what this vector is, well this vector by definition is $\beta_0 v + \beta_1 Tv + ...$ and so on. So, it is just a question of writing this out etcetera. Now, I try to act $p(x)$ on this this vector $q(x)v$ right.

So, how does how does $p(x)$ act on this vector well, it is α_0 times this whole vector . So, I plug this whole vector in here ok $+\alpha$ let us write that down here $\alpha_1 T$ acting on well that same vector, this vector, $+\alpha_2\ T^2$ acting on the very same vector and so on right dot dot dot.

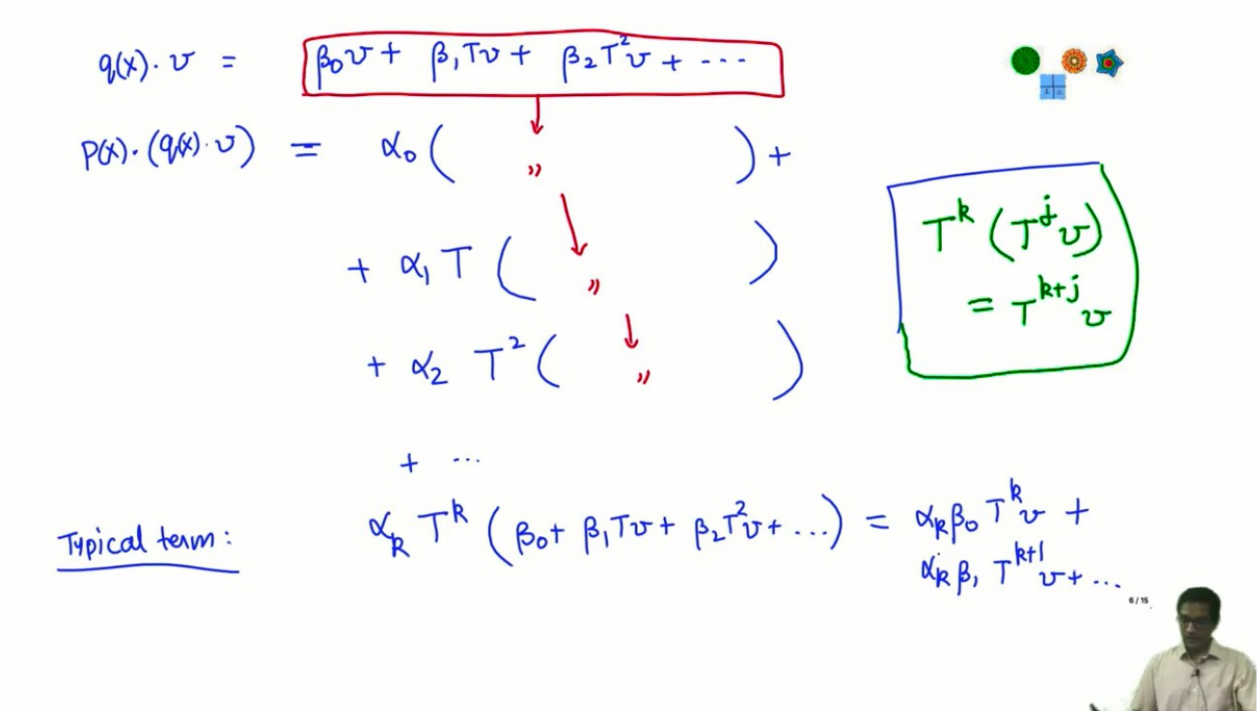
So, that is my right hand side $p(x)$ acting on $q(x)$ of v is just $\alpha_0 + \alpha_1 T + \alpha_2 T^2 + ...$ acting on that whole thing and so on ok. Now, we we can sort of so, let us take$_1$representative term and see what is going on and that will sort of tell us what to do in general. So, now, observe for example, if I take a typical term.

So, what does a typical term look like? So, typical term in this in this summation looks like. So, let me take the kth term it looks like $\alpha_k T^k$, acting on that vector in in the inside which is , $(\beta_0 + \beta_1 Tv + \beta_2 T^2 v + ...)$ and so on.

Now, when I act a T^k on a combination of vectors which each of which is you know $Tv, T^2v, T^3v, ..$ and so on. I just have to observe make the following observation, that write this here $T^k(T^j(v)) = T^{k+j}v$. So, this guy here will just become $\alpha_k \beta_0 T^k v + \alpha_k \beta_1 T^{k+1} v + ...$ and so on ok.

So, that will become the whole expansion ok. Now, that is I just written out the general term there, now you can sought of see what what goes on, if you just go back and and plug it in you will observe the following that $(p(x)q(x))v$ acting on v is in fact nothing, but this sum over all k's α_k.

$$(p(x)q(x))v = \sum_{k=0}^{deg(p)} \sum_{j=0}^{deg(p)} \alpha_k \beta_j T^{k+j} v$$



So, let let it is a double sum now K runs over all the possibilities K 0 to whatever the degree of p is whatever the top limit is β j, j again runs from 0 to the degree of q. So, let me say K to the degree of p, this runs to the degree of the polynomial q, $\alpha K \beta$ j and what do I get here T to the $K+$ j acting on v ok.

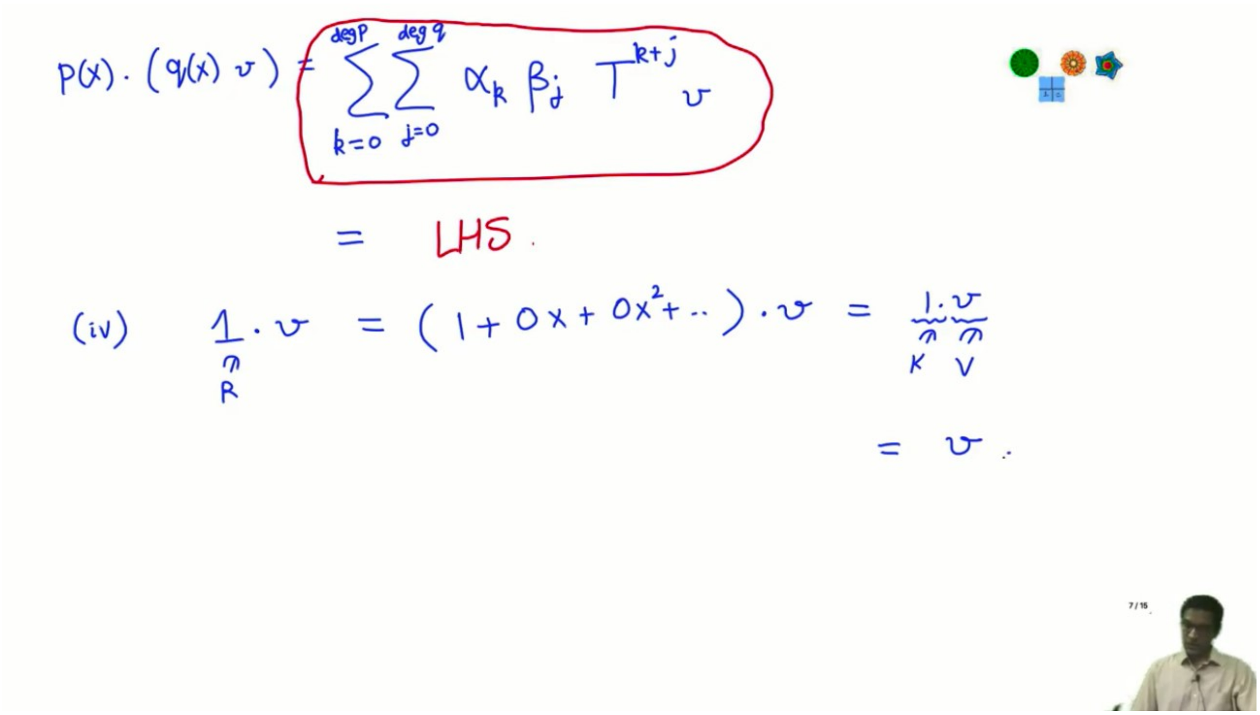
So, I I have just said the typical term the K th term I have sort of shown you what it looks like it looks like this. But, then to do the entire sum I need to also allow K to vary from $0_1 2$ 3 and so on. So, I am just doing the whole whole thing in one go so, that is my answer ok.

But, observe that is exactly what we got when we took the product of α of p and q. So, observe what is this; this answer here $p(x)q(x)$ on v the typical term here is exactly $\alpha_k \beta_j$ and the power of T in front is is $k+j$ ok. So, observe this is nothing, but you know this looks like the sum α let us say α I β j i. So, what does a typical term look like this is this is the coefficient. So, so I should say $p(x)$ so, let us write this out also as a summation.

So, this looks like, if I want to know what is the coefficient of some T to v let us call this K may be K j. If, I want to know what is the coefficient of T to the i v, then this is the sum overall k and j such that $K+j$ equals I ok this. Now a sum I going from 0 to whatever the degree of pq is ok.

Now, so, I will just leave it for you to nail down the final details. So, observe this final term here, that I have which I get when I take the product K is actually the same as the term I get here ok. So, those two answers are actually the same. So, this is the same as the left hand side that I obtained earlier ok. So, that was slightly lengthy, but completely elementary just from the definition itself .

And, let me check the final axiom axiom iv, which says that if I take the identity element of my ring and I scalar multiple it with any vector I should get back that vector. But, observe the identity element of the ring here is nothing, but well what is the identity element it is



just this polynomial right. I should think of it as this polynomial, $1 + 0x + 0x^2 + ...$ and so on acting on v and that by definition is just $1 \cdot v$. This is the usual scalar multiplication.

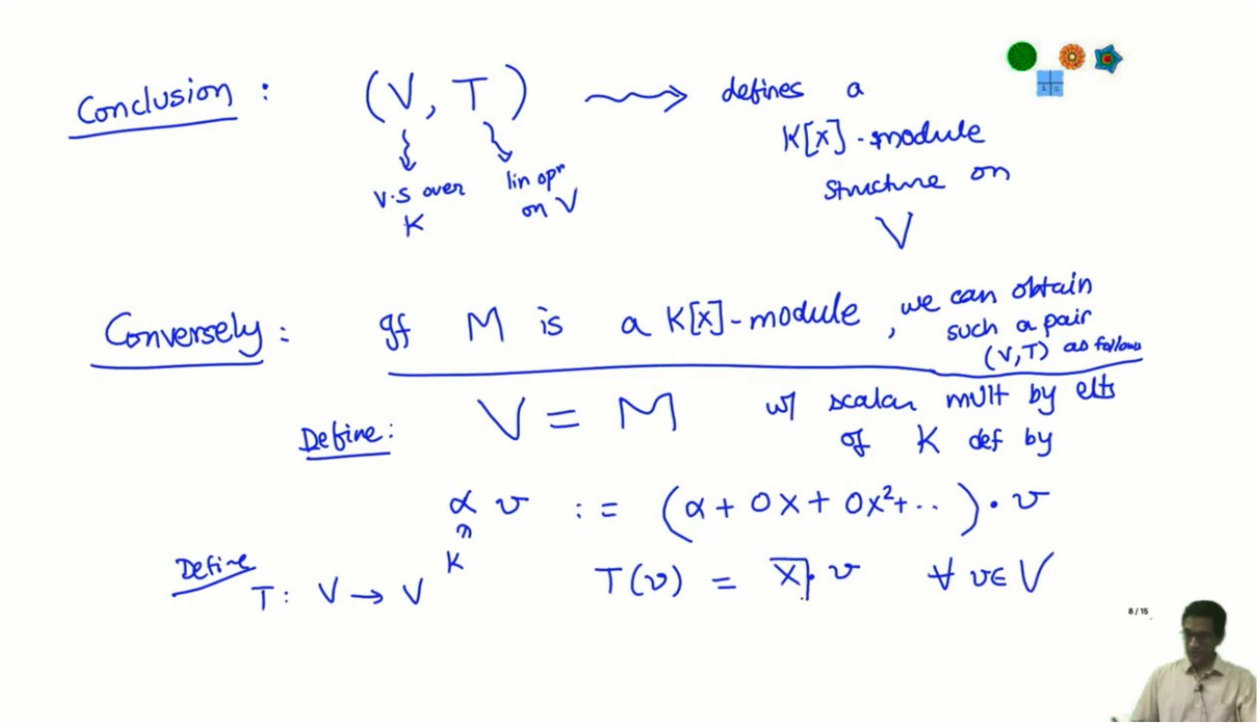
And, then the rest of the terms do not contribute, because I get zeros in front ok. So, this is now just a usual scalar multiplication. So, this one is in K, this is an element of v and this is the scalar multiplication in the vector space V and there of course, we know the answer is v ok. This is by the axioms of the vector space. So, what I get is that $1 \cdot v = v$ by the fact that v is a vector space over K ok.

So, what have we managed to do we have managed to show that all the 4 axioms hold in this case ok. So, we have therefore, shown the following. So, conclusion is the following, if I give you a pair of a vector space over K together with a linear operator on that vector space ok .(V, T) is a vector space over a field K and T is a linear operator on that vector space.

Then, this pair gives me the structure this allows me to define defines a $K[X]$ module structure on my vector space V ok. And, in fact the converse is also true that if I am given a $K[X]$ module, then from that I can extract a vector space and a linear operator ok. So, let me quickly tell you what the converse is. So, suppose I am given a $K[X]$ module conversely, if V is a $K[X]$ module, may be we will call it m let us call this M.

Suppose, M is a $K[X]$ module, then from this M I can extract a vector space and a linear operator as follows, if M is a is a $K[X]$ module observe that the constants. So, I can define the vector space as follows . So, let us define define a vector space V, as follows I will take V to just be the the set M itself with scalar multiplication as follows, with scalar multiplication by elements of K right. I have to make it a K vector space I can I can do this.

So, if M is a $K[X]$ module, we can obtain such a pair V comma T as follows, that is what I am trying to do construct a vector space and a linear operator on it. Ah. The vector space is just the same as the space M itself, but now I want to think of it I may tell you how to do scalar multiplication by elements of K M. Well you just say the following say I want to take

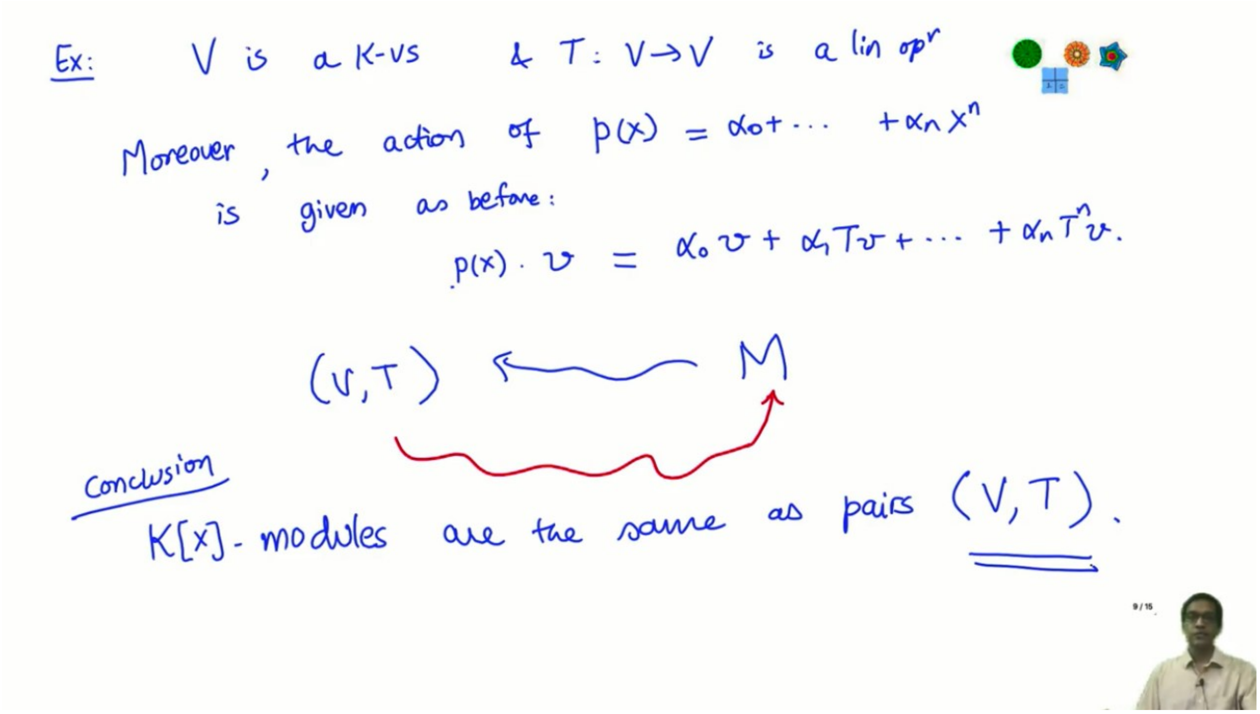


an element v in M and I want to figure out, how to scalar multiple it with a scalar coming from K right. How should we define this is a question. And, the answer is well a scalar is just a constant polynomial right. I can think of this scalar for example, as just this you know think of it as constant is alpha, constant term is α and and all the other coefficients are 0s. So, scalar is a particular example of a polynomial just a constant polynomial. So, take that constant polynomial and you act on v ok.

And, what do you mean by act on v I am after all given that M is a $K[X]$ module right. So, I am given an action of $K[X]$ on M, in particular I am given an action of all the constant polynomials. So, that is all I am saying define the action of the scalar α on V, as just the action of a constant polynomial α on v ok. So, that is my definition. And, my linear operator T from V to V is obtained as follows, define the linear operator T by saying T acting on v is just the action of X on v ok.

So, X remember is again a polynomial it is a very special polynomial, the degree$_1$homogeneous polynomial x power 1. I just look at how x acts on v ok. That again is given because V is after all given to be a $K[X]$ module, M is given to be a $K[X]$ module. So, I just use the given action. So, T v is defined like this X v ok. This is for all v in V . So, X is my my special polynomial here ok. So, given a $K[X]$ module I can get these two pieces of information; one I can define a vector space over K, which is the same underlying set M, but in which the scalar multiplication is just the same as the action by the constant polynomials. And, I can get a linear operator from this action T, I can get a linear operator T from this action as follows, I just take the action of the special polynomial X on this this module ok.

And, what you now I have to check which I will leave as an exercise. So, exercise to check that V is in fact, a K vector space and T is in fact a linear operator . And, moreover the action of any polynomial $p(x)p(x)$ is sort of given by the same as same prescription as before is



given as before meaning this polynomial $p(x)$ acting on v will just be $\alpha_0 v + \alpha_1 Tv + ... + \alpha_n T^n v$ ok.

In other words, if you started with this pair so, so on the one hand I I took M and from M I have constructed a pair (V, T) right. Now, we have already described a way of of starting with a pair vT and constructing a module from it ok. Now, what we are saying is that these two are really inverse processes of each other ok. If, I am already given a module to start with, I extract the V and the T from it. Now, having gotten this pair I can construct a module out of that by our pervious formula. By doing that just gives me back the same module M ok. So, again this is like our pervious principle that abelian groups and z modules are the same thing.

Similarly, here the principle the the final conclusion is the following slightly loosely stated fact, that $K[X]$ modules are the same as pairs V comma T ok. And, where V is a K vector space and T is a linear operator on K ok. So, these two things are the same.

So, of course, the study on the right hand side is of a linear operator on a vector space is really the the the the key thing, one does in linear algebra right. So, this is really this belongs in linear algebra. And, in some sense many theorems from from linear algebra can be fruitfully obtained or studied from the point of view of modules ok. If you study modules over rings in particular module over the ring $K[X]$. What you actually get as a corollary is some you know nice facts about linear operators acting on vector spaces ok .