Algebra - I

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

Lecture 57 [Problem solving]

Let us do some problems. So, here is the first problem. So, suppose I have a finite group G. So, let G be a finite group, and let K be a field, ok. So, recall this notion of the group ring or the group algebra that we talked about. So, the group ring is just; what is it? Well, it is all elements of the form some linear combination, some coefficients c_g , with some basis elements 1_g . You can think of it as a vector space over the field K, c_g is coming from scalars K ok.

$$K[G] = \{\sum_{g \in G} c_g 1_g | c_g \in K\}$$

But the interesting thing as we saw is that this is a ring and it is got multiplication which is well one way of describing it, is to say if I take these two basis vectors 1_g and 1_h , they multiplied it give me the element 1_{gh}, ok.

So, this is a ring. So, recall this whole business of opposites. So, recall what the opposite of ring was. So, if I have a ring R not necessarily commutative, then R^{op} is a new ring. Well,

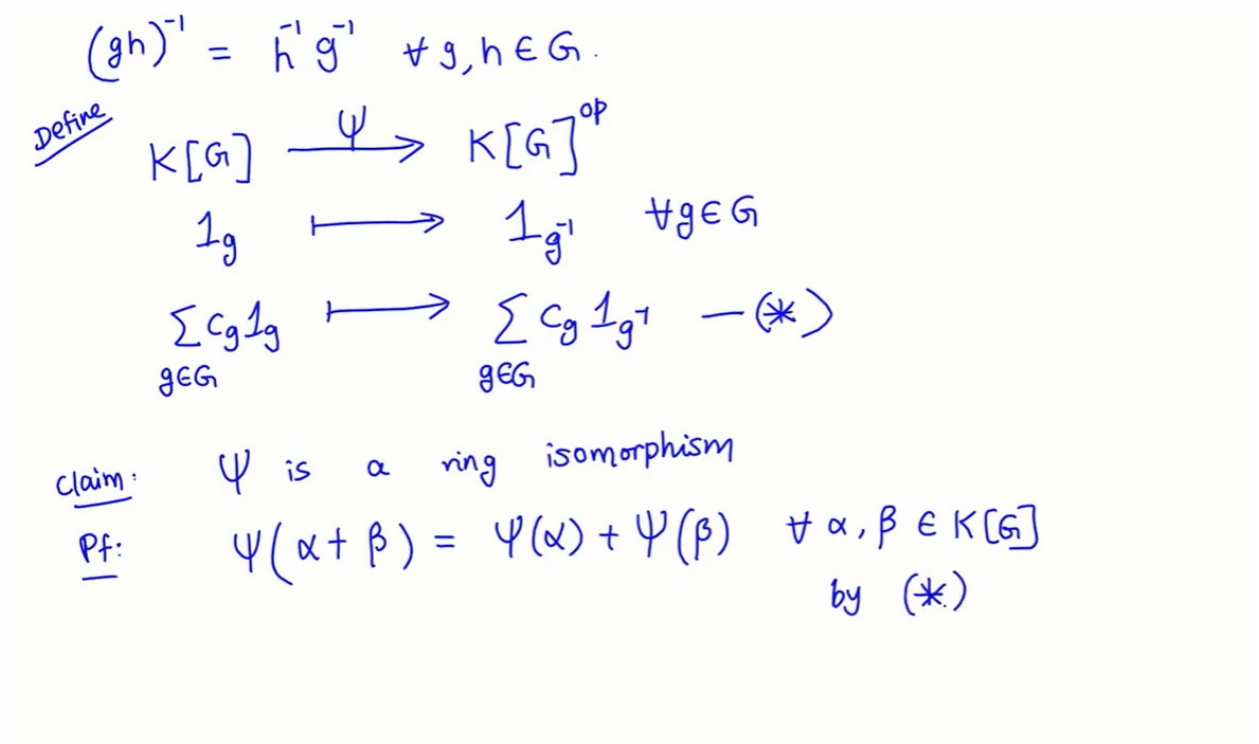
① G finite group
K field

$$K[G] = \left\{ \sum_{g \in G} c_g 1_g : c_g \in K \right\}$$

$$1_g 1_h = 1_{gh}$$

R $R^{op} = R$ as a set
same $+$ as R
$a \odot b = ba$

PT: $K[G] \approx K[G]^{op}$.



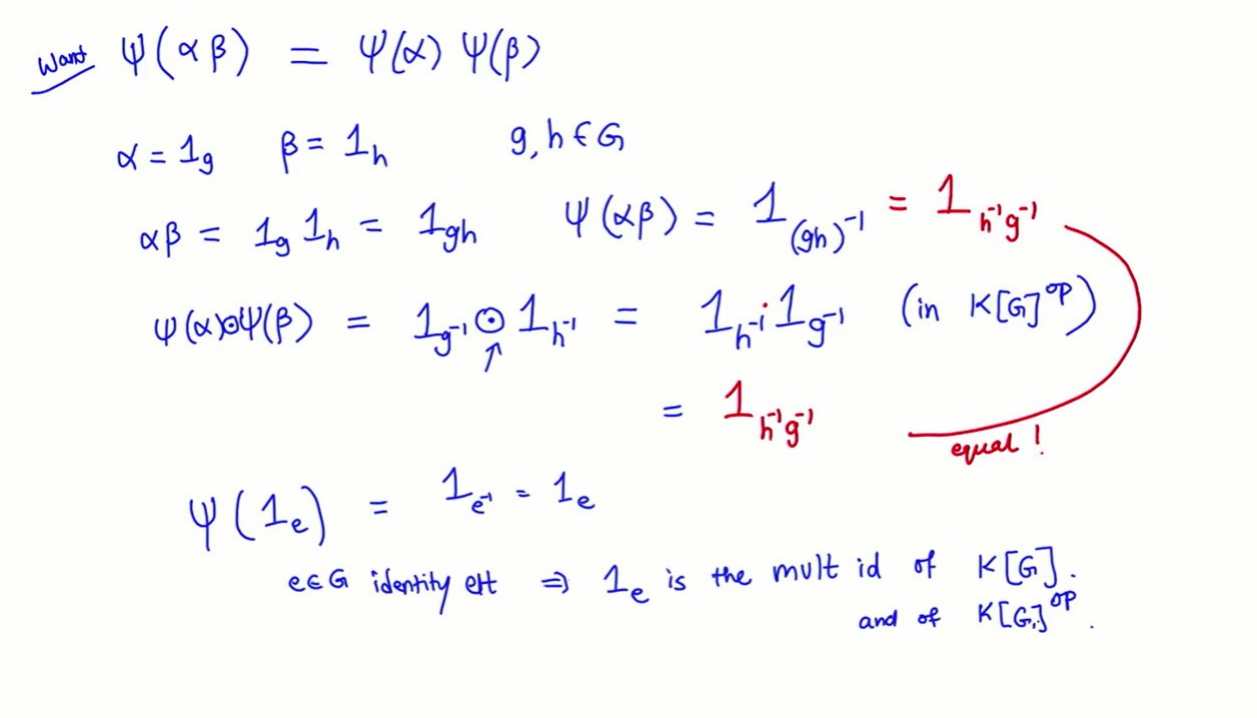
what is it? Well, it is firstly, R as a set, in fact, its R as an abelian group as well the same plus. So, I will say same plus as R but the multiplication alone is the opposite.

In other words, the new multiplication $a \odot b = ba$ in R^{op} , is just defined as the product ba in R ok. And we saw an example of the matrix ring which was isomorphic to its opposite because there was this transpose map right, A going to A^T transpose for A matrix. It sort of changes the order of multiplication right. So, that gives you an isomorphism between the matrix ring and it is opposite. So, the first problem now is to show that the same is true of $K[G]$, ok. So, prove that $K[G] \cong K[G]^{op}$ is isomorphic to its opposite. So, this ring and its opposite ring are isomorphic to each other. So, in this sense it shares this property with the matrix ring, ok.

So, let us see what we would do as in the case of matrices the key point is to somehow try and guess what the the map must be, something which you know interchanges the order of um multiplication. And in the case of groups, so recall there is this important property of groups that if I take the inverse of a product then that has the effect of changing the order, right. This is true if I have two elements of the group G and, so that somehow the the clue, we define the following map. So, here is the isomorphism. Let us define a map from the group ring $K[G]$ to itself.

As follows we take the basis element 1_g to the basis element $1_{g^{-1}}$, ok for all g in G. Of course, if I define it on the basis on a general element it is defined just as a linear combination right. So, summation $\sum_{g \in G} c_g 1_g$, therefore, what I mean is that the map does the following it takes this to $\sum_{g \in G} c_g 1_{g^{-1}}$, for all G ranging over the group G, ok.

Now, the claim is that this this map is a isomorphism between $K[G]$ and $K[G]^{op}$ set, sorry. So, what is on the other side is I am thinking of it as the ring $K[G]^{op}$ and I claim is that this this map ψ is an isomorphism. So, let us check all the properties.



Claim, ψ is a ring isomorphism. So, we need to check it preserves addition and multiplication. So, addition is easy, ok. So, because in or the level of vector spaces it is just a vector space, it is a linear transformation of vector spaces right. So, summation $\sum_{g\in G} c_g 1_g$ goes to $\sum_{g\in G} c_g 1_{g^{-1}}$, so ψ preserves addition it is easy to check. So, $\psi(\alpha+\beta) = \psi(\alpha) + \psi(\beta)$ for all α, β coming from $K[G]$. So, I will leave this for you to check. All you have to use is this equation star by star, ok because both α and β will have such expressions and you write everything out.

The key point that needs checking is really this multiplication. So, if I take a product of two elements, if I take $\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$ right. Well, I mean I wanted to be $\psi(\alpha)\psi(\beta)$ in $K[G]^{op}$ I want this, right. So, let us just check it on the basis elements.

So, let us take α to be the special element 1_g , β to be the element 1_h , ok fix two elements g and h from G. Let see whether this is at least true on um the basis elements. So, when I compute $\psi(\alpha\beta)$. So, first $\alpha\beta$ becomes 1_g into 1_h which by definition is 1_{gh} and therefore, ψ acting on this element by definition was just $1_{(gh)^{-1}}$ right. This is how ψ acts. Now, on the other hand let us compute $\psi\alpha\psi\beta$. Remembering that we are doing this this multiplication inside $K[G]^{op}$, so maybe I will just put that funny symbol for multiplication to remind us that we are actually in the ring $K[G]^{op}$. Let us go back for a second, so noticed that the right hand side is $K[G]^{op}$.

So, I take $\psi(\alpha) \odot \psi(\beta)$. What is this? Well, $\psi(\alpha)$ by definition is 1_g and I need to do this multiplication in $K[G]^{op}$ with 1_h . So, what is sorry sorry $\psi(\alpha) = 1_{g^{-1}}$, $\psi(\beta) = 1_{h^{-1}}$ right because α has 1_g , ok.

But now remember this is this multiplication is in the opposite ring which means it is the usual multiplication but in the opposite direction. So, this is because everything is taking place in $K[G]^{op}$, and now we are done, because that by definition. So, now, these two things

are equal because let us check $1_{(gh)^{-1}}$ by definition is $1_{(gh)^{-1}}$ in the group is $1_{h^{-1}}1_{g^{-1}}$ is also equal to $1_{h^{-1}g^{-1}}$, ok.

Because this is now the multiplication in the ring R right. So, I have already done the opposite. So, I interchange the order of the factors and then I do the usual multiplication on the ring R ok. So, these two are of course, equal. So, we are done, ok. And of course, third property you need checks that ψ of the the identity is the the identity, so recall that the identity of of I mean the multiplicative identity of this ring is 1 sub the identity of the group, ok. So, e is now the identity of the group, identity element, right, This is the multiplicative identity. So, if e is the identity element of the group then 1 sub e is the multiplicative identity of the ring of the ring K of G.

So, now let us compute ψ of 1 e by definition is 1 sub e $^{-1}$, but of course $e^{-1} = e$, ok. So, $\psi(1_e) = 1_e$ So, notice that 1_e is a multiplicative identity of $K[G]$ as well as of $K[G]^{op}$, um because the identity is always a two sided identity right. So, whether you multiply it on the left or the right it does not matter, it gives me the same, it it it serves the role of an identity, ok. So, I hope that is clear.

So, what we have established is that this ring $K[G]^{op}$, if G is a finite group the group ring is actually isomorphic to its opposite, ok. And what does that mean? Well, as a consequence of this thing we will probably see later that right modules for $K[G]^{op}$ and left modules of $K[G]$ are the same thing, ok.

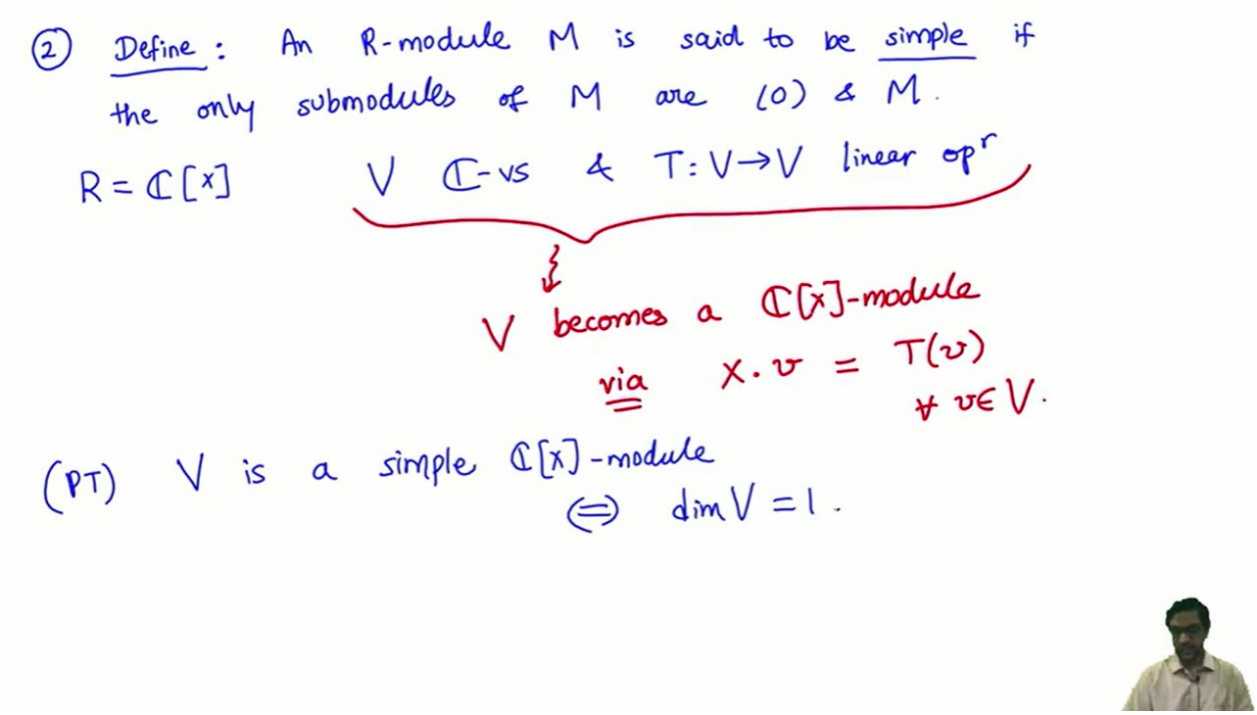
So, in if your ring is $K[G]$, then right $K[G]$ modules and left $K[G]$ modules are really the same thing because you can use this isomorphism to take a you know a a left module over $K[G]$ and convert it into a right module over $K[G]^{op}$, sorry; a left module over $K[G]$ why are this isomorphism becomes left module over $K[G]^{op}$, but a left module over $K[G]^{op}$is just a right module over $K[G]$, ok.

So, this in in essence the the conclusion or corollary of this isomorphism is that for $K[G]$ left and right modules are really equivalent notions. We do not need to worry about left versus right, ok. Let us move on to problem 2, which is again let us define a notion for this problem. So, define an R module M is said to be simple is said to be simple, ok or a simple R module, if it has no sub modules, if the only sub modules of M sub modules of M are the two obvious ones 0 and M itself, ok. So, these are the only two sub modules. Then we say R is simple, ok, it has no other non-trivial sub modules. So, now, here is the question.

So, let us do the following. Let us take the ring to be $\mathbb{C}[X]$, $\mathbb{C}$ is the complex number, $\mathbb{C}[X]$. So, as you seen in the lectures is a a module over $\mathbb{C}[X]$ is the same as a vector space over $\mathbb{C}$. So, let me take a vector space. So, let V be a complex vector space and let T be a linear operator on it, ok. And we have seen that this this data is the well what does this this data enable you to do, it it makes V into a $\mathbb{C}[X]$ module, so using this V becomes a $\mathbb{C}[X]$ module.

And what is the the additional thing? You really need to specify how x acts and what we said is that the action of x on any vector is given by the the operator T that you fixed, right. So, this was we call how we make I mean every $\mathbb{C}[X]$ module is of this form, ok. So, I fix a $\mathbb{C}[X]$ module, ok.

In other words, I fix complex vector space and a linear operator and think of V as a $\mathbb{C}[X]$ module. Prove that this is simple, prove that V is a simple $\mathbb{C}[X]$ module, if and only if the dimension of V is 1, ok. So, need to prove that the only way in which V can be a simply simple $\mathbb{C}[X]$ module is if its dimension is 1, ok. So, let us let us prove this. One direction is



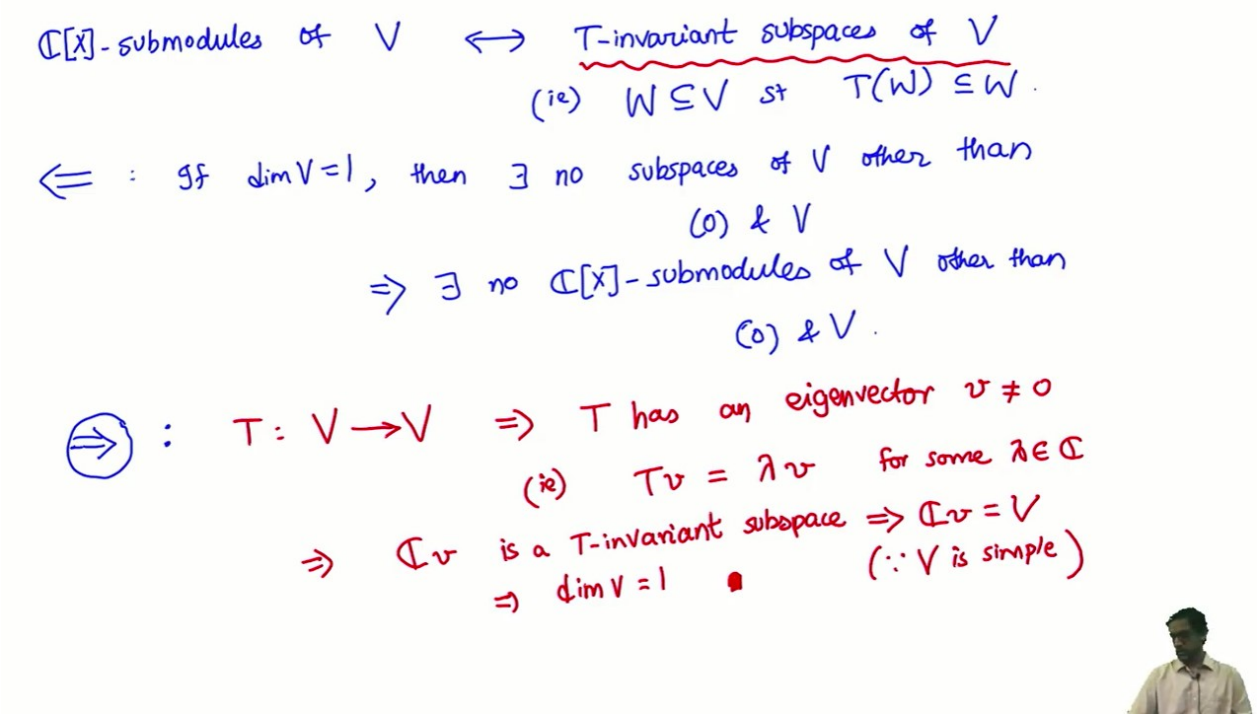
easy if the dimension is 1, then V is necessarily simple because recall what do sub modules look like.

So, first observe the following $\mathbb{C}[X]$ sub modulus of V are the same thing as T invariant sub spaces. So, these are just subspaces T invariant subspaces of V a i.e subspace W of V which has the property that T maps into itself. This is what T variant subspace means, ok. So, if the dimension of V is 1, so now, let us prove one direction.

So, let us prove this direction. If the dimension is 1, then of course, there are no subspaces other than 0 and the whole, then there exists no subspaces, not even talking about some modules here there are even no subspaces of V other than 0 and 1, 0 and the whole, ok. So, of course, there cannot be any you know further sub module. Sub modules are subspaces with an additional property. But there are no subspaces even. This is 0 and the whole, so of course, there are no sub modules. So, there exists no sub space sub modules even. There exists no $\mathbb{C}[X]$ sub modules of V other than (0) and V

So, this is trivial. It is the other direction that we need to work on. So, if it is simple, ok you have given that it is a simple $\mathbb{C}[X]$ module, then you need to show that the dimension has to be 1, ok, ok. Now, let us just analyze what a sub module is. So, you given it a simple right which means that it has no $\mathbb{C}[X]$ sub modules other than 0 and the whole. What is the sub module? It is just a T invariant sub space, right. So, what you have given is that this subspace V sorry this um complex vector space V has no T invariant subspaces, right, that is what is given other than 0 and the whole, ok.

But here is an interesting property of a complex vector space. So, I am thinking of everything here as a finite dimensional complex vector space maybe I should have said that, um let V be a finite dimensional. So, in this case I mean, ok, so let V be finite dimensional, finite dimensional complex vector space, ok and I am given T let $T : V \to V$ be given, ok.



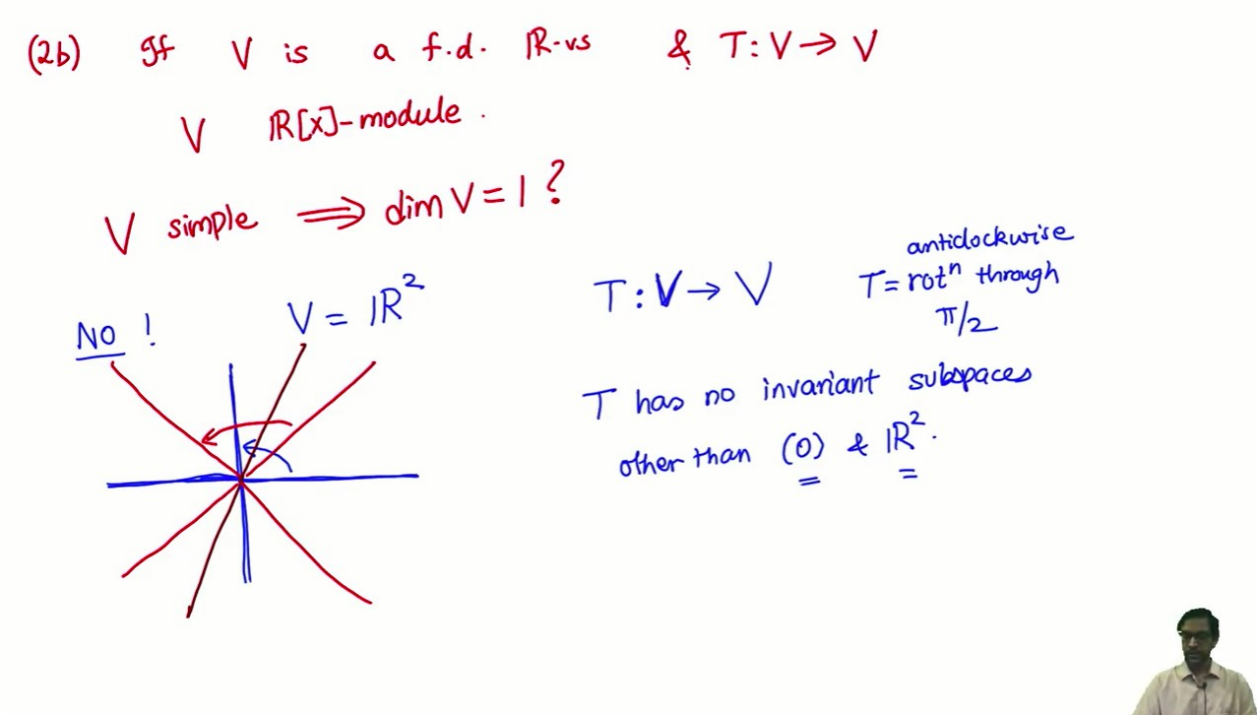
So, $T : V \to V$ is a linear operator, V is a finite dimensional complex vector space, then here is one thing I know it always has an eigenvector, ok. So, observe this just implies that T always has an eigenvalue and an eigenvector, right. At least one eigenvector is is guaranteed to exist. Now, so recall this fact from linear algebra. Now, what does that mean? Let us give that eigenvector a name. Let us call it V So, V is some nonzero vector. When $Tv = \lambda v$ you just get some multiple of V right, for some λ which is what we call an eigenvalue for some $\lambda \in \mathbb{C}$.

Now, observe that the fact that when T acts on V you get a multiple of V just means that the span of v. So, look at the complex span of V So, I will just write it like this C V is T invariant, it is a T invariant subspace. This is a T invariant subspace of V ok. But the given hypothesis says that there are no T invariant subspaces other than 0 and the whole.

But we have clearly you know constructed at least one T invariant subspace here. This is not 0. It is not the 0 space. So, the only thing it can be is is the whole. This implies that $\mathbb{C}v = V$ had better be the whole space, ok. Why? Since, V is given to be a simple $\mathbb{C}[X]$ module. This is the given hypothesis, ok.

And now you have done because you have shown that V is just the span of a single vector which means its dimension is exactly 1, ok. So, that that is the end of this proof, ok. Great um. Here is an interesting follow up question; is the same true over R the ring of real numbers, the field of real numbers, ok. So, suppose I took, um you know I took my ring to be $\mathbb{R}[X]$ and I took a real vector space. So, remember I use the fact that there are it is a complex vector space, so it has an eigenvalue and eigenvector and so on.

So, here is sort of follow up questions call it question problem 2 b, does this hold over the real numbers. So, if V is a finite dimensional real vector space and T from $V \to V$ is some linear operator that is given and we we think of V as an $\mathbb{R}[X]$ module, where x acts via the



operator T So, then the question is V is simple, suppose V is simple, does it imply that the dimension is 1? Ok.

So, observe the same prove does not work anymore because um I do not necessarily have you know eigenvalues anymore I do not have real eigenvalues anymore. So, which means that I cannot necessarily produce an eigenvector and therefore, the same proof will not work. But the question is is the result too nevertheless can you somehow give a different proof of this fact.

Now, it turns out the result is not true in this case, ok. So, here is the the interesting observation. No, this is not true. The simple module need not have dimension one if you are over the real numbers. And what is a what is a very easy example? Well, we we can just take V to be a two-dimensional space, ok.

So, I just look at this two-dimensional real vector space R 2. And I take this linear operator $T : V \to V$ to be, well I can I can just describe it geometrically let us take T to be the the map which is rotation through 90 degree angle, through $\frac{\pi}{2}$ angle, say an anticlockwise rotation by a 90 degree angle, ok.

So, what is it do? It rotates the plane by 90 degree. So, which means for example, the x axis here maps to the y axis under the action of this operator T ok and so on. So, any any other line that you pick. So, if you took this line here for example, say at 45 degrees it will get rotated to the line which is at 135 degrees and so on, ok. Now, this is a linear operator, ok as it is easy to check. And here is the interesting fact, this linear operator has no T invariant subspaces, ok. This operator T has no invariant subspaces other than 0 and the whole, ok.

Why is this? Because well the total dimension is 2, this is a 0-dimensional sub space, this is the two-dimensional sub space. What else can it have? If at all it had invariant subspace it must be a one-dimensional space right.

So, the question is can T have a one-dimensional invariant subspace. What is the one-dimensional subspace? It is just a line, ok. So, the question is if can I just draw a line somewhere and say, ok, so let us say this one here I draw a line now and say; let us just use some other color. So, this is a line, can this line be T invariant? Well, what does T do to this line? It does not map this line back to itself, it maps it to the line which is you know at a 90 degree angle to this one, ok.

So, just from the geometrical definition of T it is clear that it cannot map any line to itself, it has to move every line and map it to a different line, ok. So, here is a counterexample if you are over the real numbers. Even though this space has dimension 2, this operator is such that you know V is still a simple module over Rx , ok. ah Let us move on to the next problem. This is problem 3 which is the following. Again about simple modules if you wish.

So, first little definition. So, suppose I have M which is an R module, and if I take an element of Mx in M then we call, so Rx by that I mean the space, what I get by multiplying x by all the scalars in R ok. This guy is called the cyclic sub module. So, this is by the way a sub module is called the cyclic sub module generated by x. It is just the sub module generated by x in some sense. So, if it is a singly generated sub module we say, we usually call it cyclic. It is a cyclic sub module generated by x, ok.

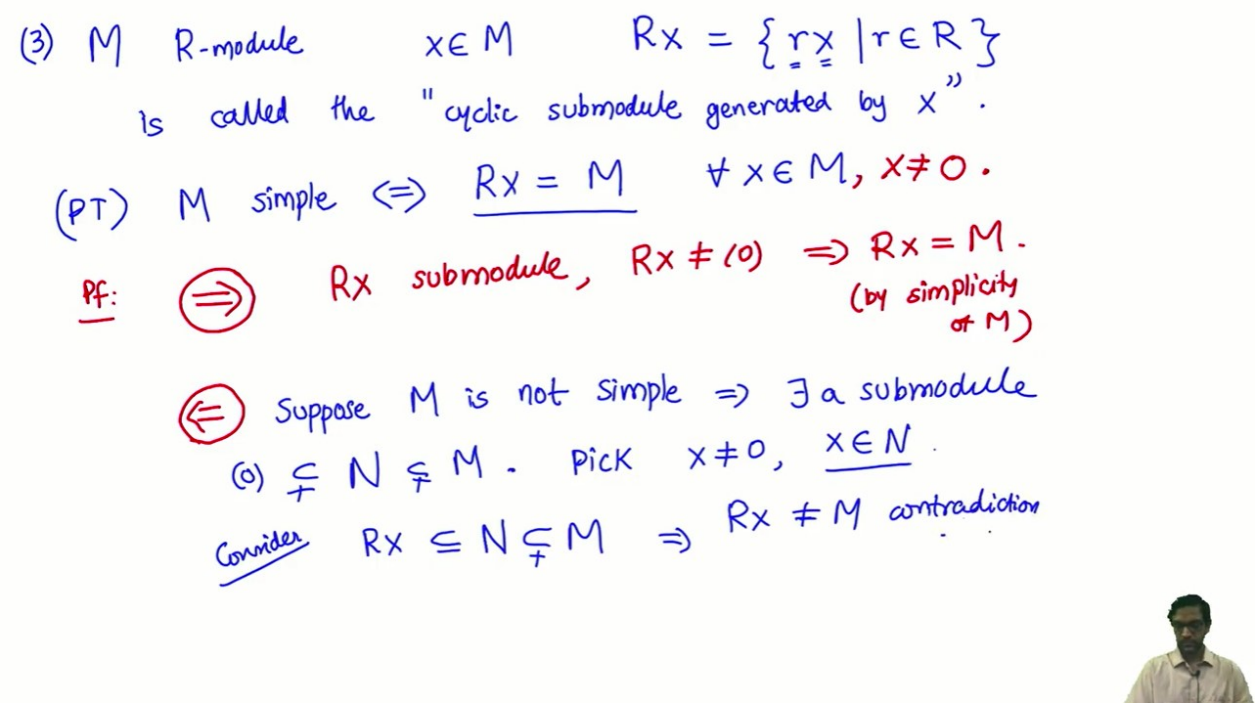
Now, here is the problem prove the following prove that M is a simple R module. Recall, from the previous problem, what that meant M is simple if and only if every cyclic sub module equals the whole module. So, by the way you should check that this is a sub module. It is a it is a easy verification. But the claim is if M is simple then every cyclic sub module has to be equal to the whole. And this an if and only if that is where the interest lies. So, let us prove this. ah One direction again it is very easy. If M is simple then recall that meant that it has no sub modules other than 0 and the whole, and here is a here is a sub module, ok. So, so I should say this is for x not 0, for all x in M other than 0, right. Of course, if I take x equal to 0 it just generates the 0 sub module.

So, if M is simple then Rx is a sub module and Rx is not 0 because I have chosen x to be not 0, therefore, Rx had better equal the whole because there are no other sub modules, ok. So, this is by simplicity of M by simplicity of N

Now, it is the converse that really needs work here, if every cyclic sub module equals the whole, why is it true that M must be simple, ok. So, let us prove that M is simple. So, what does that means? Suppose not; so, why do not we we proceed by contradiction. So, suppose M is not simple suppose M is not simple; that means; what does that imply? That means, I can find the sub module. There exists a sub module N um of M such that N is neither 0 nor the whole. So, it is sort of strictly properly between these two ends.

So, there exist a sub module N which is neither 0 nor N From this I need to get a contradiction somehow, ok. So, let us do the following. So, since N is not 0, let us pick an pick an element a nonzero element from N So, pick x not 0 x in N ok. So, take a nonzero element of N and consider the cyclic sub module generated by that nonzero element look at Rx , ok, consider Rx .

Now, what do we know? Every cyclic sub module supposed to be the whole module M but since x comes from N and N is a sub module, right. What does it mean? If you multiply x, so x is from N and I multiply x by any scalar the answer is again in N because N is a sub module, ok. So, observe if I take the cyclic sub module generated by Rx , because x is in N and N is a sub module Rx is a sub of N ok. But N is N is not the whole space N is a



strict subset of N So, this means in particular that this cyclic sub module Rx cannot equal M and that is a contradiction, ok. And that contradiction proves what we wanted.