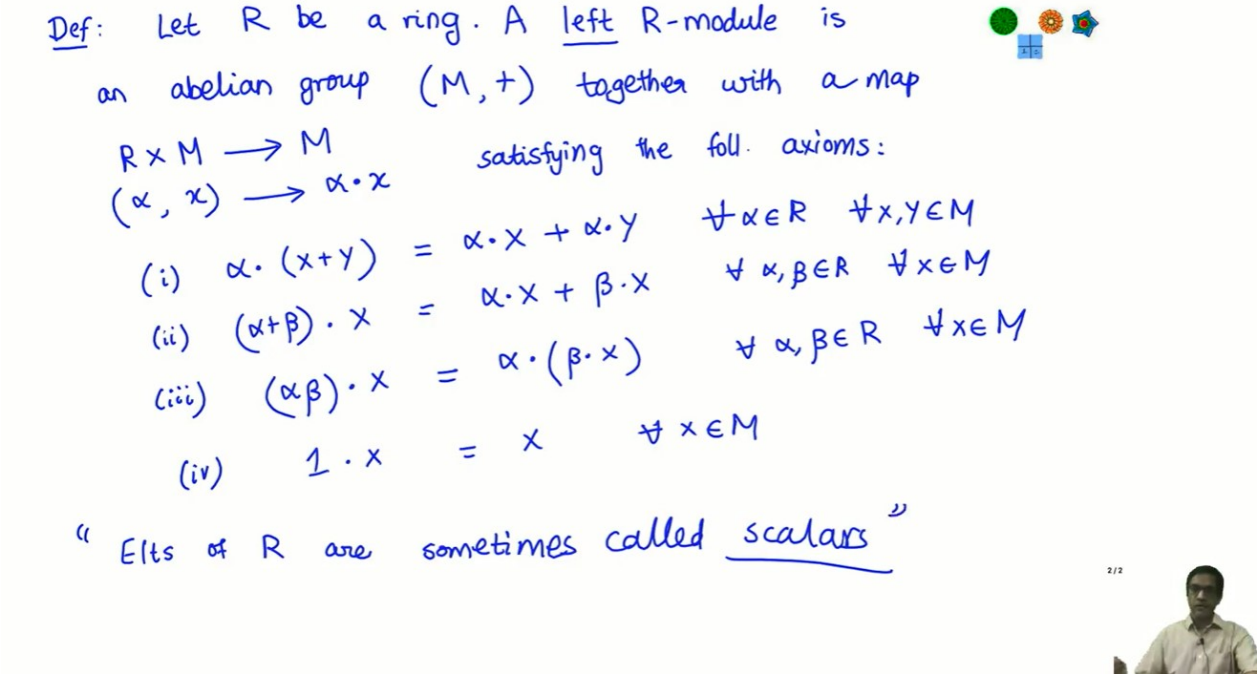
Algebra - I

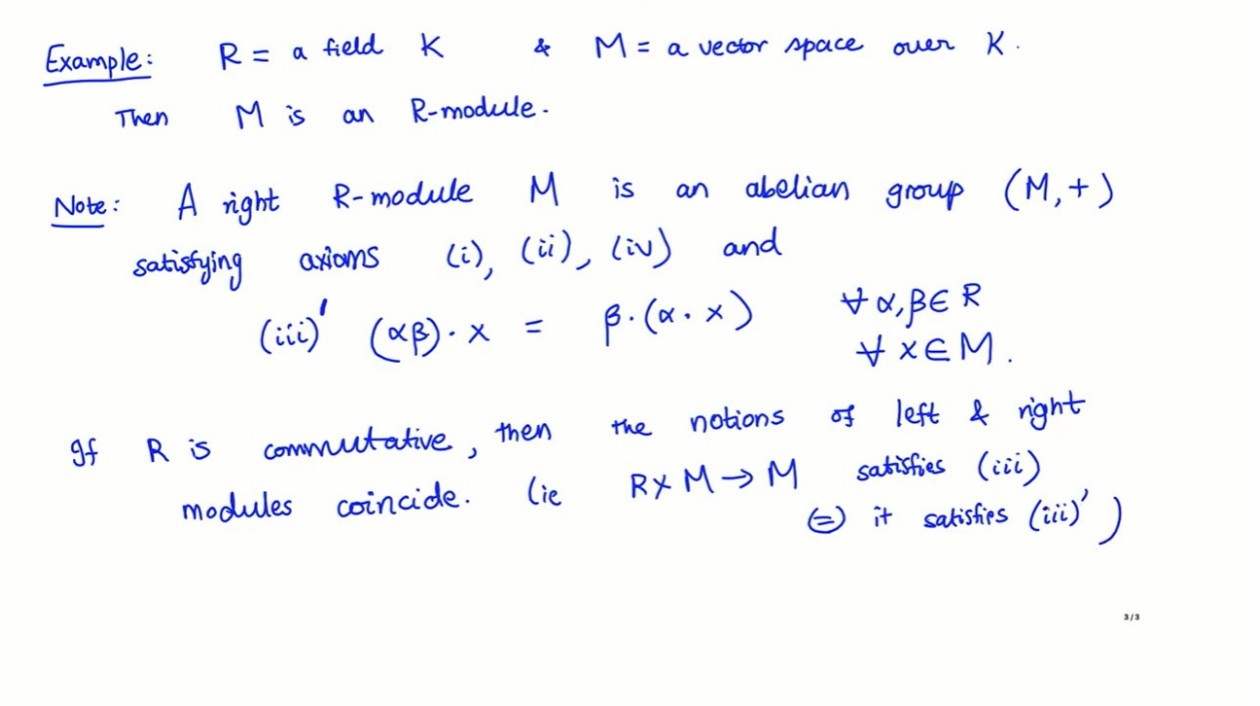
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

1. Lecture 51 [Modules: Definition]

Today, we will start an important topic; this is the notion of modules, it is a unifying notion, it captures many different things that we have seen under one single umbrella. So, let me give you the definition first. So, what is a module? So, to define a module, what we need is a ring; so here is the definition .

Let R be a ring; so not necessarily commutative, a left R module . So, remember we have encountered this notion of left and right ideals before; so when ring is not commutative, one often has to distinguish between these two notions. So, in this case we will call this a left R module that is what I am going to define; is the following, is an abelian group first; it is an abelian group . So, let me call it $(M, +)$ and let us denote the group operation $+$; so it is commutative, together with a map ok. So, this map is from $R \times M \to M$ ok. So, we write given an element $\alpha \in R$ and $x \in M$, let us denote the image of this map by $\alpha \cdot x$ ok; satisfying the following axioms.





So, satisfying the following axioms ok; axiom number i says when I take α and combine it with $X + Y$; $\alpha \cdot (X + Y) = \alpha \cdot X + \alpha \cdot Y$ and this holds for all $\alpha \in R$ and for all X and Y coming from M, its property one. Property ii says if I look at two elements of the ring α and β ; then $(\alpha + \beta) \cdot X = \alpha \cdot X + \beta Y$ for all $X \in M$. So, these are sorts of some sort of distributive properties.

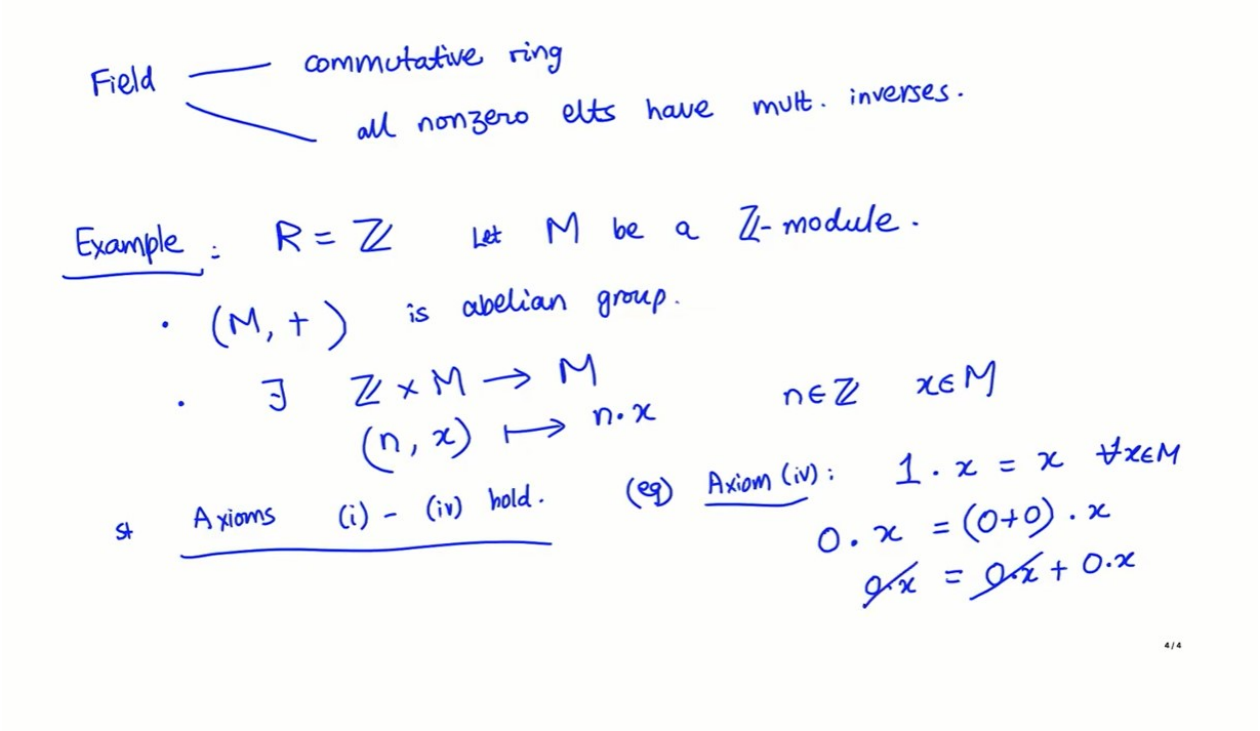
Property iii says if I multiply two elements α and β of the ring; so their product is again an element of the ring. I multiply them and then act on X, then $(\aleph\beta) \cdot X = \alpha \cdot (\beta \cdot X)$; this is for all α, β in the ring R and for all X coming from M.

And finally property iv is the identity; if I take the identity element, the multiplicative identity of the ring and look at that$1 \cdot X$, then the answer is X and this is true for all $X \in M$ ok. So, those are the four axioms which this map $R \times M \to M$ is supposed to satisfy ok.

Now, this set R; the elements of R, so let me just say this is supposed to remind you of something that you must have seen before. So, elements of R are sometimes called scalars ok and this map from $R \times M \to M$ is sometimes called scalar multiplication ok; so of course, that should ring a bell. So, observe that this is in fact exactly; it looks a lot like the definition of a vector space and in fact, that will be our our first example.

So, immediately one observes that this definition is really motivated from the definition of a vector space ok. So, example let us take R to be a field; a field, so now, let me call it K. So, K could be the field of real numbers, complex numbers, finite fields whatever.

So, I take a field K and let M now denote a vector space over this field ok ok. Then observe that these axioms are exactly what it means for M to be to be a vector space ok; so then observe M is an R module . So, the axioms of a module are exactly the axioms of a vector space when R is is a field ok; so that is our our primary example. Now, here is a small remark; so I defined left modules instead of right modules ah.



So, let me also tell you how you would define a right module. So, a right module; right R module M is again an abelian group ok. So, let us say with the + operation; satisfying well, almost the same axioms as before. So, axioms i, ii, iv, but not iii and instead of iii; they have an axiom which is now called iii; iii′. So, let us just go back and look at what axiom iii said; $(\alpha\beta) \cdot x = \alpha \cdot (\beta \cdot x)$.

Now, iii′ is the following, if we take the product of two scalars α and β and act it on x; then I demand that the answer should be β acting on $\alpha \cdot x$ ok. $(\alpha\beta) \cdot x = \beta \cdot (\alpha \cdot x)$. So, this is what it it means for a module to be a right module rather than a left module that the sort of the the order of α and β is is interchanged ok.

Now, observe that if the ring is commutative; so if R is a commutative ring; then well these two notions are really really the same, if R is commutative; then observe that the notions of left and right modules coincide ok. In other words, a left module over R would also would automatically be a right module and a right module would would automatically be a left module ok; that that map $R \times M \to M$ actually satisfies both iii and iii dash, if R is a commutative ring ok; that is what we mean. In other words, the map from $R \times M \to M$ satisfies the axiom iii; if and only if it satisfies the axiom iii dash.

And you can you can check this quickly, all you have do is just take instead of $\alpha\beta$ here I; I can replace $\alpha\beta = \beta\alpha$. So, same thing because R is commutative and then observe that axiom iii dash would just reduce to axiom iii ok. So, write out a formal proof of of this fact ok. So, so far we have defined the notion of a module and realized that it is actually nothing, but a vector space in disguise. You can sometimes say a module is like a vector space over an arbitrary ring rather than over a field ok ok.

Now, a field remember is very special kind of a ring; a field has two important properties, number one; it is a commutative ring ok commutative ring and the second important

property is that all non zero elements have multiplicative inverses; all non zero elements have multiplicative inverses right. So, these are the two important properties that the field possesses.

A general ring of course, does not have either of these properties; typical ring can be non commutative and even if it is commutative, no reason for it to have inverses right. So, you have already seen many examples of rings of both kinds. So, of course, the the theory of modules over an arbitrary ring is is much richer ok.

So, the ring does not necessarily have to; have these these special properties and so the the class of examples the the kinds of properties you get and so on; everything is now is now a much richer setting ok. So, let us look at the first example of a module which is not over a field ok; in other words let us look for a module which is not a vector space ah. So, here is example over a non field, let us take R to be the ring of integers ok. So, let us ask what is a module over the ring of integers mean? Well, if I take; so let M be a $\mathbb{Z}$ module, let M be a $\mathbb{Z}$ module; so let us try and see what that means, ok.

So, first property recall; that means, that M is an abelian group; its got an addition operation and with respect to that it is an abelian group. And the second part of the definition said that there should exist a map; so there exists a map from $\mathbb{Z} \times M \to M$, this is the scalar multiplication map; if you will which is if I take a pair $(n, x) \to n \cdot x$, this is the scalar multiplication of x by the integer n .

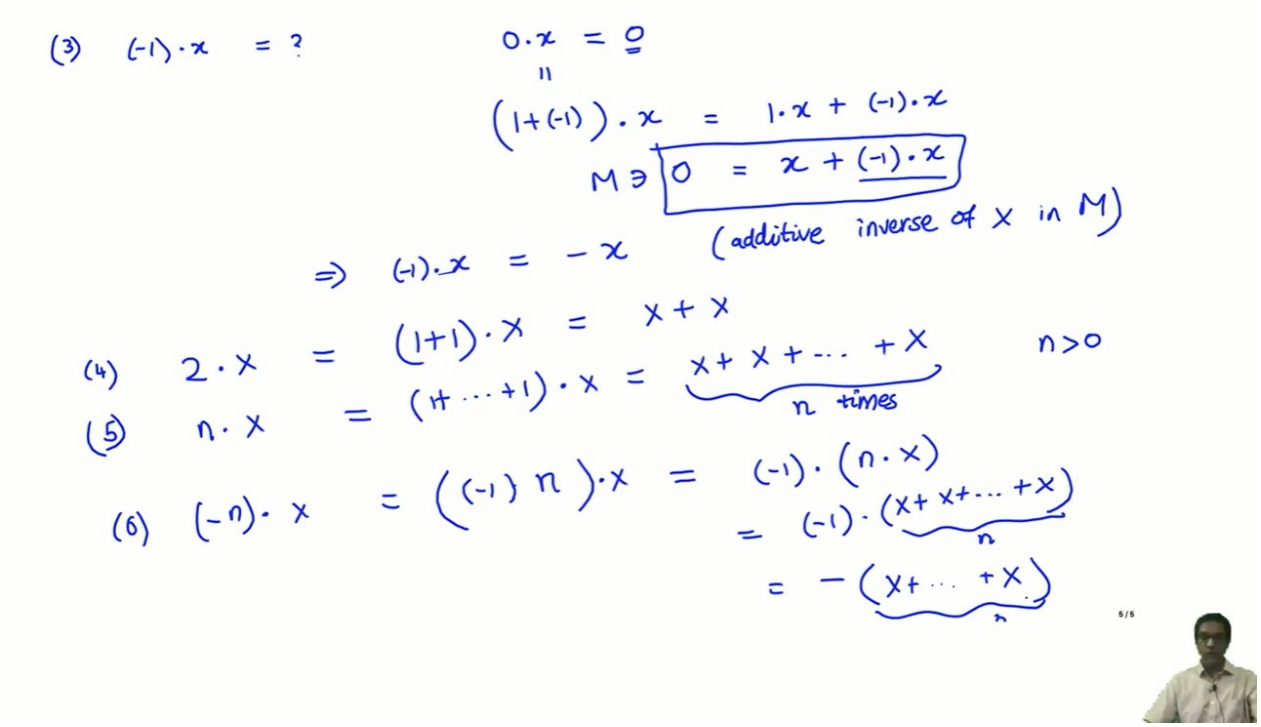
So, n is in ok; satisfying various axioms right. So, let us look at such that certain axioms hold i through iv hold ok. Now, these axioms actually impose rather severe restrictions on what this map can actually be ok. For example, let us look at axiom iv; so here is axiom iv which says if I take the multiplicative of identity of my ring which in this case is the number 1 and I scalar multiply it with any element x, then I should get x ok . So, I know this already by axiom iv that $1 \cdot x = x$ ok.

Now, we can quickly find out many other things from this; let us look at $0 \cdot x$ ok; what do you get if you multiply x by a 0? Ah In fact, these two in in arbitrary modules; so what is this? Well, as always this is; so you must have seen this calculation many a times, also in previous courses. If I try to compute 0·x, I can write it as $(0 + 0) \cdot x$ and then use the second axiom; axiom ii which is sort of a distributivity axiom which says this is nothing, but $0 \cdot x +$ $0 \cdot x$.

So, $0 \cdot x = 0 \cdot x + 0 \cdot x$ in the module M and of course, the module M is an abelian group. So, I conclude; so this is what I conclude and of course, in this abelian group, I can cancel these two elements. In other words, I can add the inverse of this to both sides and thereby conclude that $0 \cdot x$ must just be the element 0 of my abelian group M ok.

So, if I found out two things already; just from the axioms $1 \cdot x$ is x, $0 \cdot x$ is 0 and let us look at a few other ones. Let us ask what is $-1 \cdot$x; so what is $-1 \cdot$x? So, observe ah; so what is -1 really? So, $0 \cdot x = 0$, but I can also write $0 \cdot x$ as right. So, 0 is just nothing, but what I get when I add $(1 + (-1)) \cdot x$ and now again I use my axiom ii, this says this is $(1 + (-1)) \cdot x = 1 \cdot x + (-1) \cdot x$ ok. Now, of course, I have already concluded that $1 \cdot x$ is x. So, here is my conclusion that $x + -1 \cdot x$ is just the element 0 of my abelian group; so this is what I conclude finally, ok.

So, this hold; so all this is now an equation in M; remember both sides of this equation are elements of my abelian group M ok. So, what does this mean? It just means that this element which I am trying to find -1 into x; $-1 \cdot x$. So, here is my conclusion $-1 \cdot x$ is

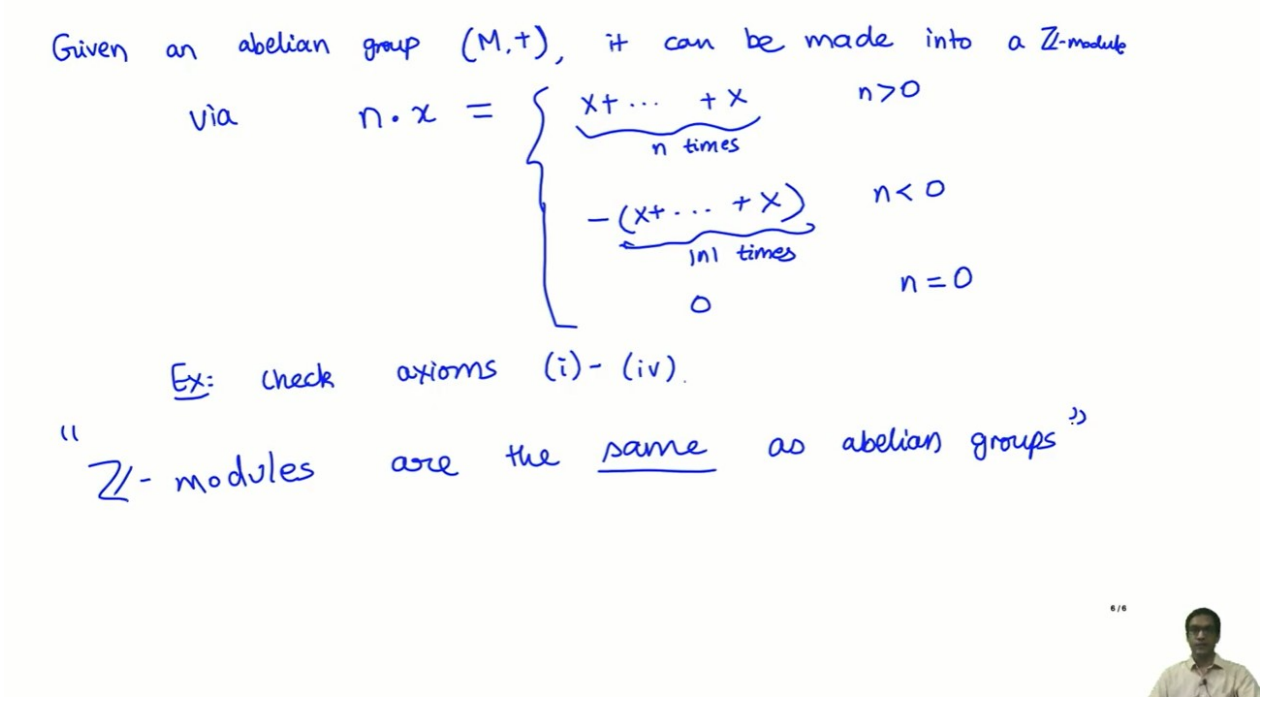


therefore, the additive inverse of x. In other words, that is the element $-x$ ok; so this is just the additive inverse of x ok.

So, I have concluded that -1 times x is just the element $-x$. Now, one can sort of keep going, you can already imagine where this is heading . So, I can compute say 2 + X; it is just (1 + 1)·X. So, 2 +X is nothing, but 1·X+ 1·X. So, it is just what I get when I add X with itself twice. More generally, if I try to take a positive number n and try to; so I have to use distributivity repeatedly, but you can check that this is what I get, its just $X + X + X$ n times ok. So, this is if n is a positive integer and from here I can also figure out what I get when I multiply by a negative number. So, this for example, so here is a quick way to do this. So, I can think of n as $-n$ as just -1 times n ah.

So, this is just the usual multiplication in the integers, this is just -1 into n, the product, the scalar multiplication with X. And this by axiom iii is just -1, acting on n·X and of course, we have already said n·x is nothing, but the element $X + X + ... + X$ n times ok. So, this is the element in M and now we have already done this right. If I take any element of my module and I scalar multiply it with (-1), it just gives me the additive inverse of that element. So, this is just $-$ of the; so, it is the additive inverse of $X + X + ... + X$ n times ok.

So, what does that mean? What have we managed to do so far, just starting with the axioms ok, we never used anything more. We have figured out that there is really only one possible map that you can define which satisfy these axioms ok. The map $\mathbb{Z} \times M \to M$ is almost forced in some sense right; n·X, I have figured out has the; has to be one of these, if if n is a positive number, then $n \cdot X$ is just add X with itself n times. If n is a or instead of n I take $-n$, a negative number then that answer is just $-$ of X added with itself n times ok. So, this this is sort of this just tells you that this is all forced in some sense; it is forced by the axioms. So, ah; so let us sort of forget this this bit of the calculation and maybe just go



ahead and define given any abelian group, you can make it into a into a $\mathbb{Z}$ module as follows. So, that is the really the conclusion here; given an abelian group M, it can be made into a $\mathbb{Z}$ module via the definition $n \cdot x$ is just either $-(X + X + ... + X)$ n times; this if n is positive or its , if n is negative ok.

Now, this has to be mod n times or if n is 0; then of course, the answer is 0 ok. So, you have to check; so now, I am giving you a definition; take any any abelian group and you define the scalar multiplication by $\mathbb{Z}$ in this manner, then this becomes a $\mathbb{Z}$ module ok; its check that it satisfies all the axioms ok. Exercise; check axioms i through iv ok and sort of conversely; what we what we just showed is that if I have a $\mathbb{Z}$ module, then in a sense that $\mathbb{Z}$ module is more or less the same data as an abelian group ok. I do not get anything extra there; the map ah; so if I have a module over Z; of course, I have an abelian group, but conceivably I could define some scalar, some strain scalar multiplication map I; maybe there are many different ways of defining scalar multiplication by $\mathbb{Z}$ right.

But what we have just shown is that; no that is not possible there is only one scalar multiplication map that you can define which satisfies all the axioms that you need to satisfy ok. So, in a sense it says that talking about a $\mathbb{Z}$ module is the same as; you know the data of a $\mathbb{Z}$ module is really the same as the data of an abelian group, it is there is no extra data there ok; so these two notions are actually identical ok.

So, what we have just shown is that $\mathbb{Z}$ modules are really the same . So, it is a slightly loose statement because what same means is is in the in the sense of our discussion $\mathbb{Z}$ modules are the same as abelian groups [noise] ok. In other words, given given a $\mathbb{Z}$ module, I can look at the underlying abelian group and given any abelian group, I can make it into a $\mathbb{Z}$ module in in this manner ok. So, that sort of our first; first example of a module which is not a vector

space ok. So, next time, we will look at another example is slightly more non trivial than this one.