


Lecture 61 [First isomorphism theorem]

Let us talk about the First Isomorphism Theorem today. Before that let me tell you what isomorphisms are. We have talked about homomorphism so far. So, what is an isomorphism of R -modules? So, suppose I have two R -modules M and N , R is some fixed ring, they are both say left modules over a given ring. A map $f : M \rightarrow N$ is said to be an isomorphism if it is well firstly, it needs to be a homomorphism. So, let us me let me phrase it like this, a homomorphism $f : M \rightarrow N$ is said to be an isomorphism if it admits an inverse, ok. So, which means there is some map g in the opposite direction, there exists g uh such that g is a homomorphism also. And f and g are mutual inverses of each other which means $f \circ g$ is the identity map on N and $g \circ f$ is the identity map on M , ok.

Now, here is a little proposition which makes it easy to check that a given map is an isomorphism. You do not really need to to you know look for a homomorphism g in the opposite direction and so on. If f is a bijection, ok, so uh proposition is the following,

Isomorphism : $M \xrightarrow{f} N$ R -modules 

A homom $f: M \rightarrow N$ is said to be an isomorphism
 if $\exists g: N \rightarrow M$ st g is a homomorphism and
 $f \circ g = id_N$ and $g \circ f = id_M$.

Propⁿ: $f: M \rightarrow N$ is an isomorphism $\Leftrightarrow f$ is a bijective
 homomorphism.

Pf: Ex. $(g = f^{-1}$ set map)



Endomorphism : $M \xrightarrow{f} M$ homomorphism
of M



$M \xrightarrow{f} M$ isom $\Rightarrow f$ is an "automorphism"

(Eg) $R = \mathbb{Z}$ $M = \mathbb{Z}$ $N = 2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$

$M \xrightarrow{f} N$
 $n \longrightarrow 2n$ is an isomorphism
 $n \longrightarrow -2n$ " " "

uh $f : M \rightarrow N$ is an isomorphism is the same as saying if and only if f is a bijective homomorphism, ok.

And bijective just means it is a one-to-one on to map of sets. So, from $M \rightarrow N$ it should it should be a bijection, and it should be a homomorphism, ok. Now, if we have these two properties, then uh that is enough to to find a map g . So, I am going to leave the checking as an exercise. Why? You know because recall if I have a bijection between these two, uh between any two sets then I have something called an inverse set map at the moment there is only a map of sets if you wish, ok which goes in the opposite direction.

But it is very easy to check that because f is a homomorphism the inverse map will also get the same properties. It will also acquire the same properties uh of a homomorphism, ok. So, you can check that easily. So, here is a little excise. A isomorphism is nothing, but a bijective map of sets which is also a homomorphism, ok. Now, uh let us also introduce two more words. We sometimes talk about endomorphisms, ok. So, what is an endomorphism? An endomorphism is a map, uh it is a homomorphism between the same spaces. So, if I have a homomorphism from a module M to itself, then we usually say this is an endomorphism of M , ok.

So, endo just means uh inside or within. So, it just maps M back to itself. So, such a map a homomorphism from $M \rightarrow M$ is called an endomorphism of M . And similarly, uh an isomorphism from $M \rightarrow M$ is called an automorphism of M , ok. So, if $f : M \rightarrow M$ turns out to be an isomorphism then we usually call this an automorphism, ok. So, these are just two more words which are used as short hands to say that both M and N are actually the same module M in those cases, ok. So, we now know homomorphisms, isomorphisms, endomorphisms, automorphisms.

Now, let us look at some examples of isomorphisms. So, if I take my ring to be the ring of integers then modules are nothing, but abelian groups. So, let us take here the abelian

Propⁿ: Let $f: M \rightarrow N$ hom. of R -modules.

Then: f is injective $(\Leftrightarrow) \ker f = (0)$
(one-to-one)

f is surjective $(\Leftrightarrow) \operatorname{im} f = N$.
(onto)

Pf.

Ex

groups \mathbb{Z} and $2\mathbb{Z}$. So, $2\mathbb{Z}$ just means the set of all even integers. This is a sub module of M , ok. But observe that even though N is a sub module of M , M and N are actually isomorphic to each other, ok. Here is an isomorphism. So, consider the map n going to $2n$, this is an isomorphism of \mathbb{Z} modules because well notice that well firstly, it is a bijection because every I mean it is clearly a one-to-one map, it is on two because all even numbers occur here.


And it is a homomorphism of \mathbb{Z} modules, because we call we said before the homomorphism of \mathbb{Z} modules is nothing, but a homomorphism of abelian groups, ok. And this is of course, a homomorphism of the underlying abelian groups \mathbb{Z} and $2\mathbb{Z}$. So, this is an isomorphism. In fact this is not the only one, you can also construct another isomorphism between these two modules which is \mathbb{Z} uh n going to $-2n$, ok that is also an isomorphism.

So in fact when two modules are isomorphic. It is not always that there is a unique isomorphism between them there are often many different isomorphisms um between two between two isomorphic modules here, ok. So, that is the notion of isomorphism. Now, two more important notions which again are things which you have seen already in the case of groups, and rings, and so on is the notion of a kernel and an image of a homomorphism.

So, suppose I have $f: M \rightarrow N$, ok. Suppose this is the homomorphism of R -modules. So, let us say both M and N are modules over a fixed ring R , then we talk about the kernel. So, this is the definition, the kernel of this map is all elements which map to 0. The image of this map is of course, just the image in the sense which is $f(x)$ as x ranges over M .

So, clearly this is a sub of N , this is a sub of M , subset of M and N . And uh here is the immediate proposition. The kernel is a sub module of M and the image is a sub module of M , ok. So, let me prove this. Well, I will prove one of them, the other is is easy, um in fact both are easy. So, let us check that the kernel is a sub module for example, ok.

So, let us take the first guy the kernel. So, what do I need to check? Well, I need to check two things to check that it is a sub module. First I need to check closure under addition. So, if I take two elements x and y in the kernel, I need to check whether $x + y$ is in the kernel 2, ok. And how do I check whether their sum is in the kernel? Well, I will act f on it and see if it gives me 0, ok. But in this case f of $x + y$ is because f is a homomorphism, this is $fx + fy$, so that is 0. So, what does that tell me? It tells me that $x + y$ is also in the kernel of f , ok.

Thm (first iso thm for modules): Let $f: M \rightarrow N$ be a 
 R -homomorphism. Then $\frac{M}{\ker f} \cong \text{im } f$ (isomorphic as R -modules)

Pf: $(M, +) \xrightarrow{f} (N, +)$ is a group hom.

\therefore By the first iso thm for groups (fund. thm for group hom)

we know:

$$\boxed{\frac{M}{\ker f}} \xrightarrow{\varphi} \boxed{\text{im } f} \quad \text{is an } \underline{\text{isom}} \text{ of groups}$$

$$m + \ker f \rightarrow f(m)$$

only remains to show: $\varphi(r(m + \ker f)) \stackrel{?}{=} r \varphi(m + \ker f)$
 $\forall r \in R \quad \forall m \in M$



Similarly, if I take x and I multiply it by a ring element r , I want to know whether rx is in the kernel, but again $f(rx)$ is just I can pull the r out, so and write it as $r \cdot f(x)$, ok. But now this is just nothing, but rx was in the kernel.

So, this is $r \cdot 0$ and we have sort of proved this once before that $r \cdot 0$ must actually be 0, ok. How do you do it? You write 0 as $0 + 0$, you expand out and so on. So, $r \cdot 0$ will be the same as $r \cdot 0 + r \cdot 0$ and so on, right. So, you you you we have seen this argument once before.

So, what does that uh lead us to? We have shown that $f(rx)$ is actually a 0 too, ok. So, which means that we conclude not only is the sum in the kernel the scalar multiplication of an element of the kernel by a ring element is also in the kernel, ok. And these two properties are exactly what it means for the kernel to be a sub module. So, the conclusion is that the kernel of f is in fact a sub module, ok.

And I leave the other one for you as an exercise. Show that the image is also a sub module, ok. Now, uh here is the other important fact about kernels and images. Again, something that just comes from groups. The map f is injective which means it is one-to-one. So, let me say what f is. f is a map from $M \rightarrow N$, uh homomorphism of R -modules. Let f be this. Then, f is injective which means it is a one-to-one map if and only if the kernel of f is 0, ok. By this I mean the 0 sub module.

Similarly, f is surjective which means it is on to, it is an on to map. So, injective is the same as saying it is a one-to-one map, surjective just says it is an onto map, this is if and only if the image is the whole space N , ok. And again, I am going to leave this as an exercise just from, follows just from the definitions more or less, ok, So, uh and again you have seen this in in the context of groups already, fine. So, now, coming to the uh to the main theorem. It is called the first isomorphism theorem. Again, this is like the first isomorphism theorems you have already seen in the cases of groups, and rings, and so on.

So, let me um give you the statement of the theorem. So, this is usually called the first isomorphism theorem for modules. So, this is for modules now. So, what does it say? It says that if I have let f be a homomorphism $M \rightarrow N$ be a R-homomorphism, then it says that M modulo the kernel of f that is the quotient module, M mod the kernel is isomorphic. So, this is a symbol for isomorphism.

$$\frac{M}{\text{Ker}(f)} \cong \text{Img}(f)$$

It is isomorphic to the uh module image of f , ok. Remember image of f is a sub module of N . It is a module in its own right, M by the kernel it is a quotient module. The claim is that these two are isomorphic as R-modules, ok. So, the M modulo the kernel is isomorphic to the image. So, that is uh as in all the earlier cases. That is the statement of the first isomorphism theorem. And in fact the proof is very quick here because we have remember we already have a first isomorphism theorem for groups, ok. So, proof recall. So, let us do the following. Let us forget the fact that M and N are modules for the moment. Think of them only as groups. They have an underlying additive group structure.

So, think of M and N as additive groups, and recall that uh a module homomorphism is in particular a group homomorphism, right. The first axiom just says that f of $x + y$ is $fx + fy$. So, I can think of this map f , firstly, as being a group homomorphism between the underlying abelian groups. And now for groups I already have the the first isomorphism theorem. So, remember the notion of kernel here is exactly how we define the kernel in the case of groups, right. It is everything which maps to the identity. But the identity is exactly 0 in this case, ok.

So, the kernel is exactly, the kernel in the sense of groups and therefore, by the fundamental theorem of group homomorphisms or the first isomorphism theorem if you wish, um first isomorphism theorem for groups sometimes also called the fundamental theorem of group homomorphisms.

So, look back on on those lectures, where this was derived by this. We conclude we know the following that we can define a map from the group M modulo the kernel of f to the group image of f , ok. These are both now the just the additive groups. There is a map between them. So, maybe I will call it something, let us call it ϕ . What is this map which is it sends $m +$ kernel of f , the coset to just the value f of m , ok. So, we know that this is an isomorphism of groups, ok. So, everything is only now for groups, the underlying additive groups, ok.

Now, what we want to show is that that very same map, the claim is that this map ϕ is in fact it is more than just a group homomorphism or uh a group isomorphism it turns out also to be an R-module isomorphism, ok. So, what does that require us to do? In addition to the group structure here what we have in M modulo the kernel is a scalar multiplication by elements of R , the same thing on the right side. So, we just have to now show that ϕ also respects the scalar multiplication. If we do that then automatically ϕ becomes a R-module homomorphism. It is already a bijective map because it is an we know it is an isomorphism of groups. We have already done that work.

So, we do not need to redo it. So, we only remains because we are appealing to the work that we have already done in proving this theorem for groups. It only remains to show one simple thing here that ϕ respects the ring the scalar multiplication. So, I need to check that when I apply ϕ to r times a coset. I need to check whether this gives me the same answer as

$$\begin{aligned}
 \text{LHS} &= \varphi(r(m + \ker f)) = \varphi(\underline{rm} + \ker f) \\
 &= f(rm) \\
 \text{RHS} &= r \varphi(m + \ker f) = r f(m) \\
 &\Rightarrow \underline{\text{proved!}}
 \end{aligned}$$

because
f is a
R-homom.

r acting on ϕ of this, ok. If I check this it means that I can pull out the ring elements r . So, I have to take this for all ring elements r for all elements m of M , ok.

So, let us just use the definition of ϕ and check what the left hand right hands will be. So, observe that the left hand side is r acting on $(M + \ker f)$ kernel of f . So, let me compute that. So, the left hand side is just r acting on this is by definition I just have to act r on the representative.

And $\phi(rm)$ by definition is f acting on rm . Let us go up here and check $f(m)$ was the definition on the map ϕ . So, here it is just f acting on the representative rm . So, similarly the right hand side was r acting on ϕ of this coset, but in this case this is nothing, but r acting on fm by definition, ok. Now, observe that r acting on fm and $f(rm)$ are actually equal to each other because f is in fact, f is a homomorphism of R -modules, ok. So, observe we started out this proof by; so, let us first say we are done now, so therefore done, proved, ok. So, that completes the proof of the first isomorphism theorem.

So, observe the way we have proved this the strategy here has been to first show that uh to to first ignore the fact that M and N are R -modules. Think of them only as abelian groups. Only think of f as a abelian group homomorphism and then do everything appeal to the group theory uh statement for the first isomorphism theorem. But then finally, after we we we have shown it is a it is an isomorphism at the level of groups we go back and now see whether we can also incorporate this additional scalar multiplication into the the picture. To do that what we finally, end up needing is this additional statement about f , that f was not just a group homomorphism it is also a R -module homomorphism, ok.

So, this is a very important statement. The first isomorphism theorem as always is uh it tells you that the images of homomorphisms can be identified with certain natural quotient sub quotient modules, ok.