

Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 07
Kernels, ideals

So, let us continue our study of ring homomorphisms. So, we have defined and looked at some important examples of ring homomorphisms. So, now, I am going to start talking about associated things to ring homomorphisms. So, let us start. So, what we will do now is talk about something called the “Kernel of a ring homomorphism”. So, you all know from group theory and when you learned about group homomorphisms there is something called kernel of a group homomorphism. So, let us do that.

So, let us look at kernel of a homomorphism. So, and the definition is exactly the same. So, before that let me actually give you an exercise, which we have essential done in our calculations earlier.

(Refer Slide Time: 01:03)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

File Edit View Insert Actions Tools Help

B / [color palette] [tools]

exercise: let $\varphi: R \rightarrow R'$ be a ring homomorphism.
Then $\varphi: (R, +) \rightarrow (R', +)$ is a group homomorphism.
Recall the kernel of a group homomorphism:
It is the set of elements that map to 0.
We use the same definition for ring homom:

So, let us say ϕ from R to R' is a ring homomorphism ok. So, here of course, I am not saying this, but R and R' are two rings; R and R' are two rings and ϕ is a homomorphism. Then, if you simply look at ϕ forget the multiplicative structure on R in other words just look at the additive group of R and R' . If you look at R and R' R to R' as a function of the additive groups, this is a group homomorphism ok.

So, if you go back to the previous video and just look at the relevant parts you will see a proof of this. By definition, $\phi(a+b)$ should go to $\phi(a) + \phi(b)$ but the other properties will ensure that $\phi(0)$ will go to 0 $\phi(-a)$ will go to $-\phi(a)$ ok. So, this is not difficult to check.

So, it is a group homomorphism. So, now recall so, this exercise for you to do so, you have to do this. So, recall the kernel of a group homomorphism. What is a kernel of a group homomorphism? It is the set of elements that map to 0 right, kernel is always the set of elements that map to 0 . So, we use the same definition here. So, this is really a set theoretic object. So, we use the same definition for ring homomorphisms. So, the kernel of ϕ so, now, this is just an aside.

(Refer Slide Time: 03:19)

The "kernel of ϕ "

$$\text{Ker } \phi := \{ a \in R \mid \phi(a) = 0 \} \subseteq R$$

Assume all our rings are not zero. In fact, $\text{Ker } \phi$ is a additive subgroup of $(R, +)$.

Is $\text{Ker } \phi$ a subring? It is not!

$\text{Ker } \phi$ does not contain 1 , $\phi(1) = 1 \neq 0$ in R' .

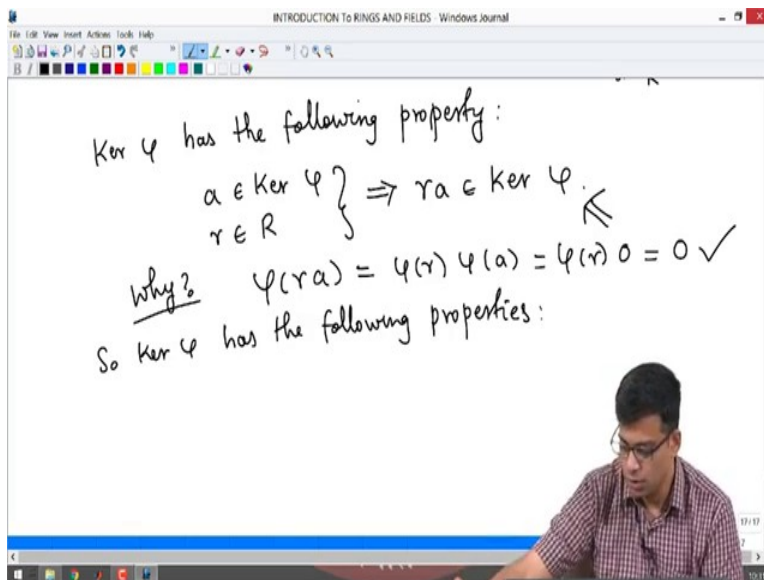
So, given ϕ from R to R' a ring homomorphism, the “Kernel of ϕ ” which is denoted by $\ker \phi$ is by definition the set of all elements of R so that $\phi(a) = 0$. So, let us focus a little bit on what kind of element, what kind of subset this is, this is a subset of R right. But, because kernel is really defined using the notion of group homomorphism, it is more than a subset. In fact, $\ker \phi$ is a subgroup. So, I am going to write additive subgroup just to emphasize the fact that we are looking at the addition on R . So, additive subgroup of R comma plus.

So, when I write R comma plus I mean I am insisting to that I am looking at R as an additive group forgetting the multiplication. So, it is an additive subgroup of R comma plus this is exactly what we have done in group theory. So, there is in other words if 0 is in the kernel, that 0 is in the kernel is the first point, if a and b are in the kernel $a + b$ is in the kernel that follows from the definition, if a is in the kernel $-a$ is in the kernel.

What other properties of now let us come back to ring theory; we are doing rings not groups. So, what other properties does kernel have? Is kernel is sub ring? Think about it for a second. Is kernel a sub ring? It is not. Why not? It is not, because remember a sub ring is a subset which is a ring by itself in particular it is supposed to contain 1 , but can the kernel contain 1 ? No, kernel does not contain 1 , because what is $\phi(1)$? By definition, $\phi(1) = 1$ and I am assuming as always that 1 is not 0 in R not prime ok.

R' prime assume always all over rings are not zero. So, there are at least two elements; 1 and 0 they are distinct elements. So, 1 is not 0 . So, $\ker \phi$ is not a sub ring. So, the analogy of with a kernel of a sub group homomorphism being a subgroup does not carry over here it is not a sub ring, but it does have nice properties in particular in addition to being an additive sub group it has the following property.

(Refer Slide Time: 06:17)



Kernel phi has the following property: kernel phi has the following property. So, if a is in the kernel what I want to say is that it is closed under multiplication, but in a strong way. It is not just closed in the sense that to multiplication product of two things in kernel is in the kernel, but product of something in the kernel by any group element is in the kernel ok. Why is this? So, why? This is very easy to check. So, what is, in order to check if something is in the kernel we have to see if its image is 0 or not. So, what is $\phi(ra)$? $\phi(ra)$ is by definition of a ring homomorphism is $\phi(r)$ times $\phi(a)$.

Now, r is an arbitrary group element. So, we do not know anything about $\phi(r)$, but we do know that a is in the kernel. So, $\phi(a)$ is 0 right, $\phi(r)$ is something, but $\phi(a)$ is 0, but $\phi(r)$ times 0 is 0, because anything times 0 is 0. So, $\phi(ra)$ is 0, so that means, ra is in the kernel.

So, it has a very strong multiplicative closure property. Take anything in the kernel; take anything in the ring not in the kernel anything even outside the kernel, the product is in the kernel. So, kernel has the following properties so, kernel has the following properties.

(Refer Slide Time: 08:09)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

File Edit View Insert Actions Tools Help

Why? $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0 \checkmark$

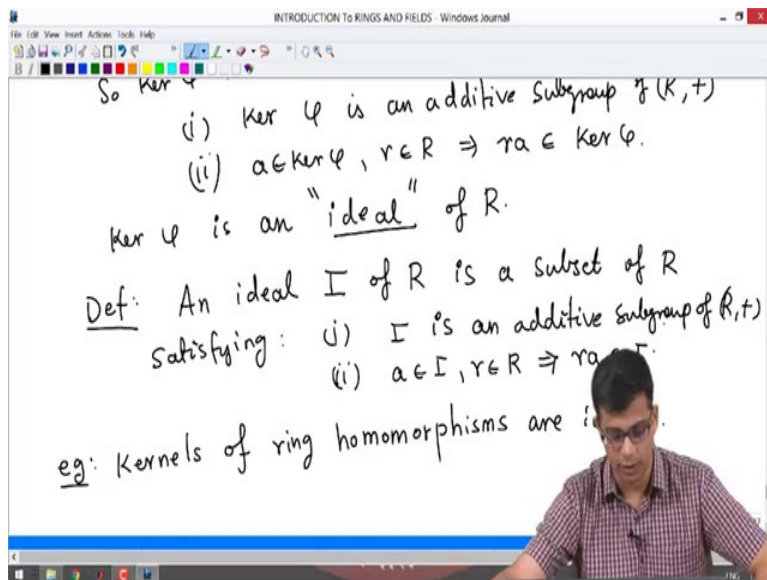
So $\ker \varphi$ has the following properties:

- (i) $\ker \varphi$ is an additive subgroup of $(R, +)$
- (ii) $a \in \ker \varphi, r \in R \Rightarrow ra \in \ker \varphi$.

$\ker \varphi$ is an "ideal" of R .

one, it is an additive subgroup of R plus, and two, if a is in the kernel r is in the ring the product is in the kernel ok. Now, we want to give a special name to subsets of a ring that have this property. So, kernel φ is a special case of that. So, kernel φ is an "ideal" ok. So, what is an ideal? So, this is a very very important word in ring theory. So, after defining rings and homomorphisms the next important thing is this.

(Refer Slide Time: 08:59)

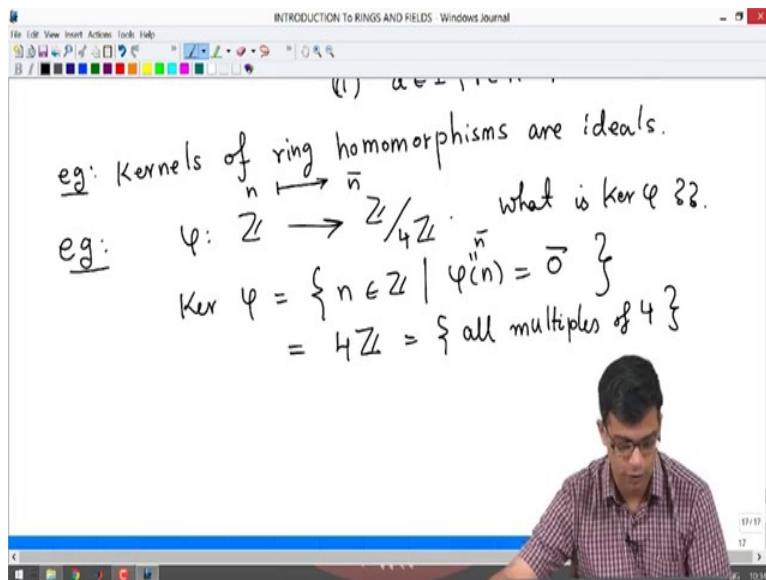


So, I will formally write the definition, it is simply the properties one and two. So, an "ideal" I of R is a subset of R satisfying. So, I am going to repeat exactly the conditions that I wrote: I is an additive subgroup of R plus. So, in particular it is not empty remember 0 must be in I . And, ii if you take an arbitrary element of I and an arbitrary element of the ring the product is also in I , ok.

So, the ideals are this and kernels of homomorphisms are ideals. In fact, kernels of homomorphisms or exactly the ideals. So, in general any ideal can be realized as the kernel of a ring suitable ring homomorphism. So, the most important examples of ideals are the kernels of ring homomorphisms ok.

So, we started with the definition of a kernel of a ring homomorphism and we noticed that it is not a sub ring, but it is what we now call an ideal ok. So, in order to understand more about ideals, let us look at some examples ok.

(Refer Slide Time: 10:35)



So, the ring homomorphism, that we looked at earlier \mathbb{Z} to $\mathbb{Z} \bmod 4\mathbb{Z}$, what is the kernel of this? What is the kernel of this? So, I claim the kernel is all integers remember kernel is a subset of the domain in this case \mathbb{Z} . So, all integers such that $\varphi(n)$ is the 0 element of $\mathbb{Z} \bmod 4\mathbb{Z}$ which is 0 bar in our notation.


So, this is precisely $4\mathbb{Z}$ right, this is simply all multiples of 4 ok. So, when does an element in \mathbb{Z} go to 0 under this homomorphism, remember this map sends n to n bar right. So, n bar must be 0. So, n bar must be 0; that means, n must be a multiple of 4. So, kernel is exactly the multiples of 4.

(Refer Slide Time: 11:45)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

eg: $\varphi_2: \mathbb{Z}[x] \rightarrow \mathbb{Z}$ Substitution
 $f(x) \mapsto f(2)$
 $\text{Ker } \varphi_2 = \{ f(x) \in \mathbb{Z}[x] \mid f(2) = 0 \}$

Recall: $R[x], \alpha \in R, g(x) \in R[x]$.
 We can divide $g(x)$ by $x - \alpha$;
 the remainder is $g(\alpha)$.



The other example that we looked at, let us say φ from $\mathbb{Z}[x]$ to \mathbb{Z} ok. So, this is the substitution map, substitution remember φ^2 is what I think we looked at. So, here $f(x)$ goes to $f(2)$, what is a kernel of this? Kernel of φ^2 is all polynomials in $\mathbb{Z}[x]$ such that $f(2) = 0$ ok.

So, now I am going to tell you ask you to recall something I talked about when I talked about division inside polynomial rings. So, recall so, in any ring R and any polynomial ring $R[x]$ if you fix α in R . Let us say so, $f(x)$ or $g(x)$ in $R[x]$. We can divide $g(x)$ by $x - \alpha$ right always divide that because $x - \alpha$ is a monic polynomial. So, we can divide $g(x)$ by $x - \alpha$ the remainder is $g(\alpha)$ right. This I have proved remainder when you divide $g(x)$ by $x - \alpha$ is $g(\alpha)$.

(Refer Slide Time: 13:27)

INTRODUCTION TO RINGS AND FIELDS Windows Journal

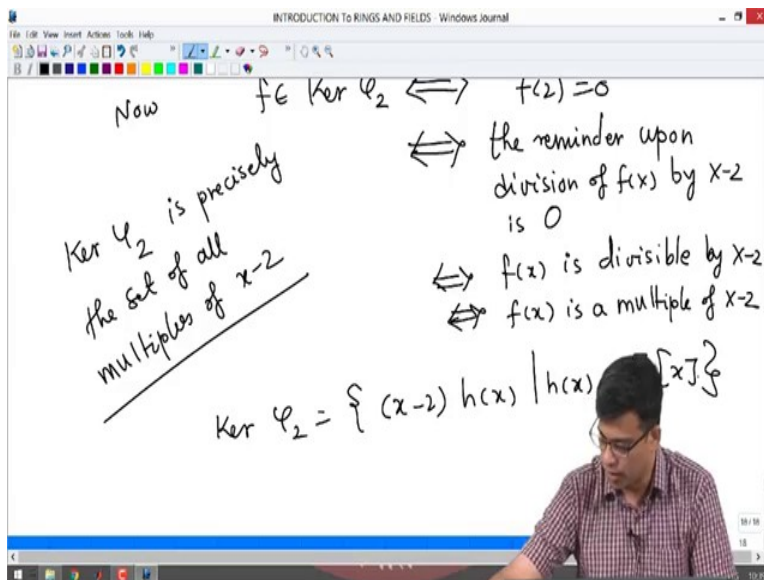
We can divide $g(x)$ by $x-\alpha$;
the remainder is $g(\alpha)$.

In our case: the remainder when we divide $f(x)$
by $x-2$ is $f(2)$.

Now $f \in \text{Ker } \varphi_2 \iff f(2) = 0$

So, now if you apply this idea to our situation in our case, the remainder when we divide $f(x)$ by x minus 2 now, in our case x minus 2 is f of 2 right. And, now if f is in the kernel, now if f is in the kernel of φ_2 then f of 2 is 0 right. So, actually I will write it like this, f is in the kernel if and only if f of 2 is 0, because that is the definition of the kernel, f is in the kernel if and only if f of 2 is 0.

(Refer Slide Time: 14:27)



That means, this happens if and only if the remainder upon division of $f(x)$ by $x - 2$ is 0 right, because $f(2)$ is precisely the remainder when you divide $f(x)$ by $x - 2$. So, $f(2) = 0$ means the remainder upon division of $f(x)$ by $x - 2$ is 0; that means, $f(x)$ is divisible by $x - 2$ that is what we say when the remainder is 0, we say that is divisible. For example, when you divide 5 by 4 by 2 the remainder is 0. So, we say 4 it is a divisible by 2. On the other hand divide 5 by 2 the remainder is 1. So, we say 5 is not divisible by 2. So, $f(x)$ is divisible by $x - 2$. So, kernel of ϕ_2 is precisely when if $f(x)$ is divisible by $x - 2$ that is another way of saying $f(x)$ is a multiple of $x - 2$ right.

So, in other words the up shot all this is kernel ϕ_2 is precisely set of all multiples of $x - 2$. So, in a I can write it like this kernel ϕ_2 is exactly $(x - 2)h(x)$, where $h(x)$ is any arbitrary polynomial of $\mathbb{Z}[x]$ right. Multiple of $x - 2$ means $x - 2$ times an arbitrary thing. So, that is how we describe the kernel of ϕ_2 . So, kernels have this nice form. So, now I want to mention as nice observations. So, this is a small lemma.

(Refer Slide Time: 16:31)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

MUL Prop

$$\text{Ker } \varphi_2 = \{ (x-2)h(x) \mid h(x) \in \mathbb{Z}[x] \}$$

Lemma: Any ideal of \mathbb{Z} has the form $n\mathbb{Z}$ for some $n \geq 0$.

Proof: Let I be an ideal of \mathbb{Z} .
 If $I = \{0\}$, then $I = 0\mathbb{Z}$; so we are done.

In the first example, that we looked at above kernel of the map from \mathbb{Z} to $\mathbb{Z} \text{ mod } 4$ turned out to be multiples of 4. So, in other words what I want now say is that, any ideal of \mathbb{Z} has the form $n\mathbb{Z}$ for some n greater than or equal to 0.

So, any ideal of the ring of integers has the form $n\mathbb{Z}$ remember what is a $n\mathbb{Z}$? So, this is the set of all multiples of n . So, that is just a short convenient notation for writing all the multiples. So, $n\mathbb{Z}$ stands for an a as a varies in \mathbb{Z} . So, I claim that every ideal has that form. So, this is a very nice result right because you cannot have strange sets becoming ideals. So, every ideal is in this form.

So, the proof is a standard proof using Euclidean divisions. So, let us quickly do this. So, let I be an ideal of \mathbb{Z} . If I is equal to 0 remember I is an additive subgroup of \mathbb{Z} . So, it must be non-empty. So, it must contain 0. If, it is exactly 0 then I is $0\mathbb{Z}$ right. So, we are done right. So, we are done.

So, please pay close attention to this, this is a very nice, simple, but an extremely important argument in ring theory and this is this sort of thing comes up all the time. So, if I is simply the just the 0 element, it is of the form $0\mathbb{Z}$ right, because 0 times n as 0 times a as a varies it is just 0. So,

we are done we have we are claiming that every ideal is of the form $n\mathbb{Z}$, if it is simply 0 then it is $0\mathbb{Z}$.

(Refer Slide Time: 18:47)

INTRODUCTION TO RINGS AND FIELDS - Windows Journal

If $I = \{0\}$, then $I = 0\mathbb{Z}$; So we are done.
Assume $I \neq \{0\}$. Then I contains positive integers.
 $-10 \in I \Rightarrow -(-10) = 10 \in I$ ✓
Let n be the smallest positive integer in I .
claim: $I = n\mathbb{Z}$.
pf. Let $m \in I, m > 0$. By choice of n ,
 $m \geq n$.

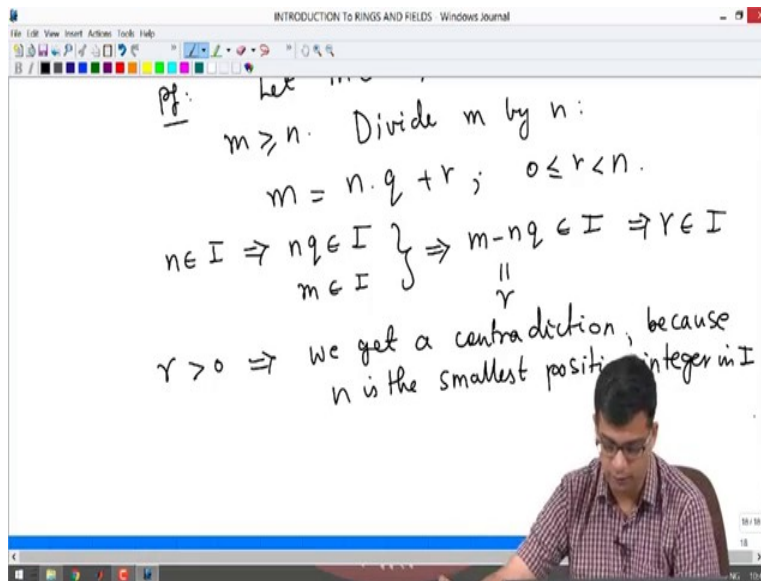
So, assume I is not the set zero. In other words I contains some other element. So, let so, first of all I claim that we can now assume. In fact, then I contains positive integers. If I contains something non-zero it contains positive integers, that is because very simple example. So, if for example, minus 10 let us say is an I .

We know that I contains something non zero, if it is positive we are done, suppose not. Let us take a negative integer, but I is supposed to be a subgroup right. So, minus of minus 10 which is 10 also belongs to I right. So, I contains a positive integer. So, I contains some non-zero integers by assumption, if you happen to pick a positive number you are done. Suppose you pick a negative number you simply take its negative. So, I contains positive integers so, that I hope is clear right; so, I contains positive integers.

Now, what I will do is let n be the smallest positive integer in I ok. I can always choose that right and I consists of some positive integers, I can I cannot pick may be the largest one, but I can always pick the smallest one so, let n be that let n be the smallest positive integer in I . Now and then choose, now I claim that I is in fact, $n\mathbb{Z}$. This n will do the job for us, I is $n\mathbb{Z}$. Why is this? So, choose let any let first take care of positive integers.

Let m be in I m positive; by choice of n , by the choice of n , m is greater than equal to n right. Because m is positive, n is positive n was the smallest positive integer containing contained in I . So, m is at least 10 .

(Refer Slide Time: 21:11)



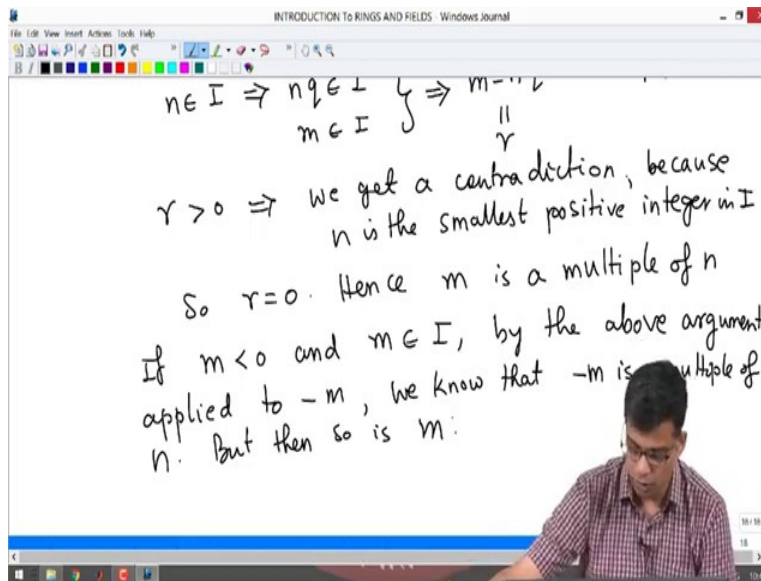
Now, divide m by n . So, what we can do is m is equal to n times q plus r , right. We can always divide m by n and we can write it like this. And, what is the property of r ? r is actually strictly between sorry r is either greater than equal at least 0 and strictly less than n .

Because, we are dividing by n the remainder will be strictly less than m ; but now notice an interesting thing, n is in I by choice; that means, nq is in I , m is in I , by also choice right; that means,

$m - nq$ is in I . Because, n is in I by ideal property nq is in I , m is in I by ideal property again $m - nq$ is in I , but the $m - nq$ is in r is equal to r so; that means, r is in I .

But, now we have a problem because, if r is positive this leads to a contradiction. What is the contradiction? What is the contradiction? If r is positive, r is strictly less than n by choice of by the process of division. So, if r is positive, because with we have then, because n is the smallest. See the contradiction is to the fact that n is the smallest positive integer in I , if r is positive r is less than n , r is smallest r is smaller than this smallest positive integer in I which is certainly absurd.

(Refer Slide Time: 23:17)

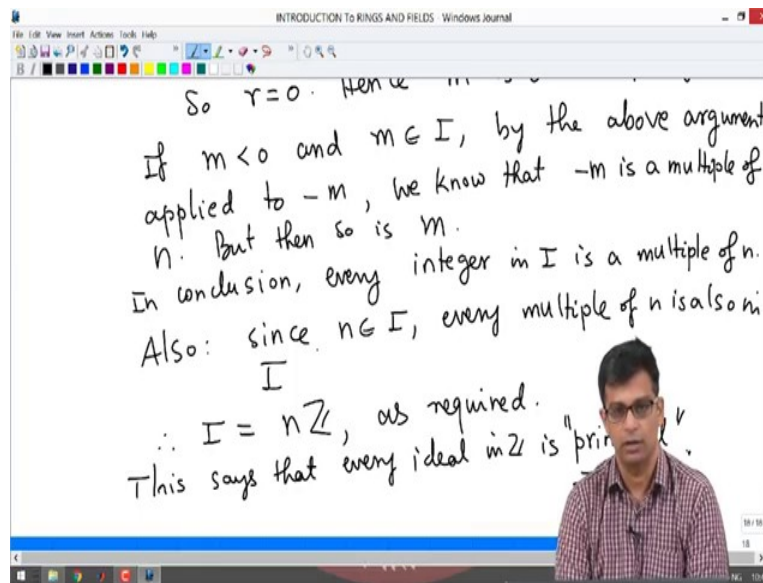


So, r must be 0. And, hence m is divisible by n which is another way of saying m is a multiple of n right. So, what we have shown is that, we have taken an arbitrary positive integer in I and showed that it is a multiple of n ok. Now, we want to say that every integer in I is a multiple of n .

Now, on the other hand if m is negative and m is in I , by the above argument, by the above argument applied to minus m right. If m is negative minus m is positive we know that minus m is a

multiple of n . But, then so, is right minus m being a positive integer in I is a multiple of n , but hence obviously, m is also because minus m is n times something m is n times minus of that thing.

(Refer Slide Time: 24:35)



So, we conclude in conclusion, every integer in I is a multiple of n . And, we also need to show that, also since n is there in I , every multiple of n is also in I right. Because, I is an ideal, if n is there, every 2 times n is there, 3 times n is there, minus n is there, minus 2 times n is there. So, I is exactly equal to $n\mathbb{Z}$, as required. This is a very beautiful argument which shows that every ideal in \mathbb{Z} is of the form $n\mathbb{Z}$.

So, we are going to talk more about generators of ideals later and talk about principal ideals. So, and at that point I will remind you this says that. So, this is just a preview of what I will do next. Every ideal in \mathbb{Z} is principal. So, "principal ideals" are ideals generated by a single element. So, I just to preview what I will do next, but I said that every ideal in \mathbb{Z} is a principal ideal generated by a positive integer n or of course 0, non-negative integer n I should say.

So, I am going to stop this video here, but in the next video or in one of the next videos, I will show that the same result holds for polynomial ring in one variable or a field so, that I will do next. So, in this video we looked at kernels of homomorphisms, we looked at what properties those kernels have and noticed that they are examples of what we defined as ideals. And, we looked at examples of ideals in various rings and in particular we showed that every ideal in the ring of integers is of the form $n\mathbb{Z}$ for a non-negative integer n .

Thank you.