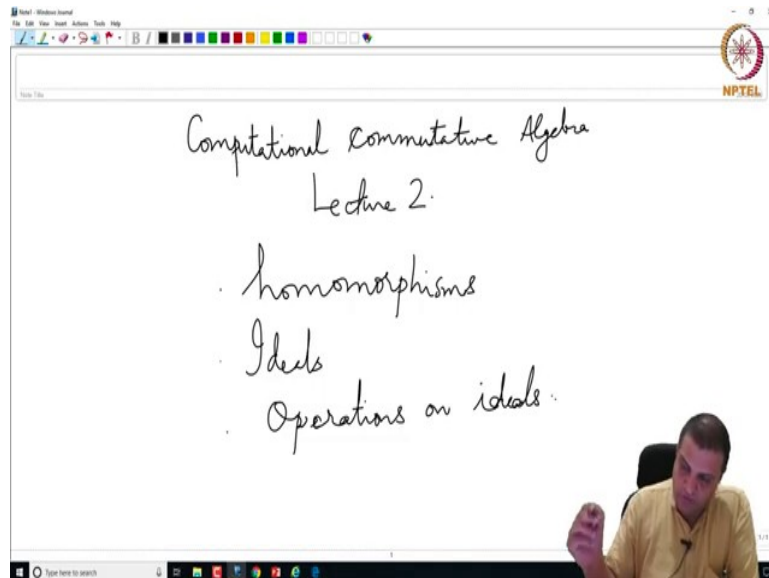


Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute

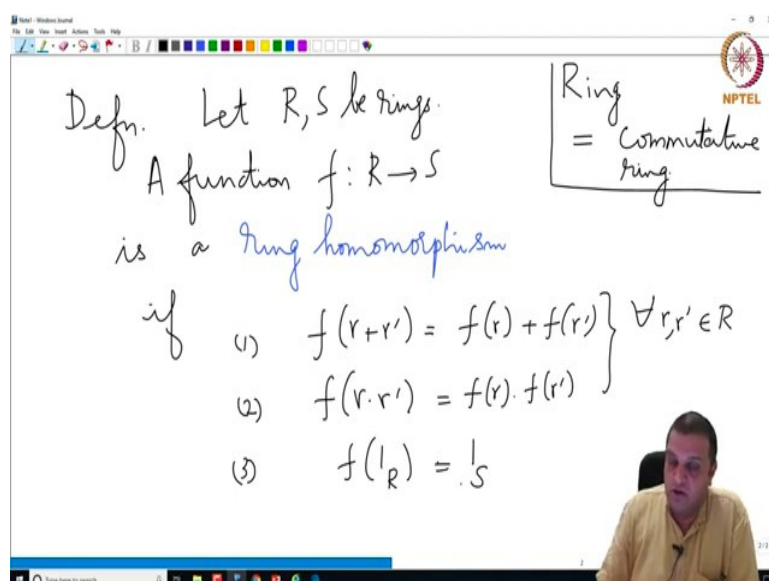
Lecture – 02
Homomorphisms

(Refer Slide Time: 00:16)



Welcome to the second lecture of Computational Commutative Algebra. So, in this lecture, we will look at ring Homomorphisms, ideals and some operations on ideals.

(Refer Slide Time: 01:00)

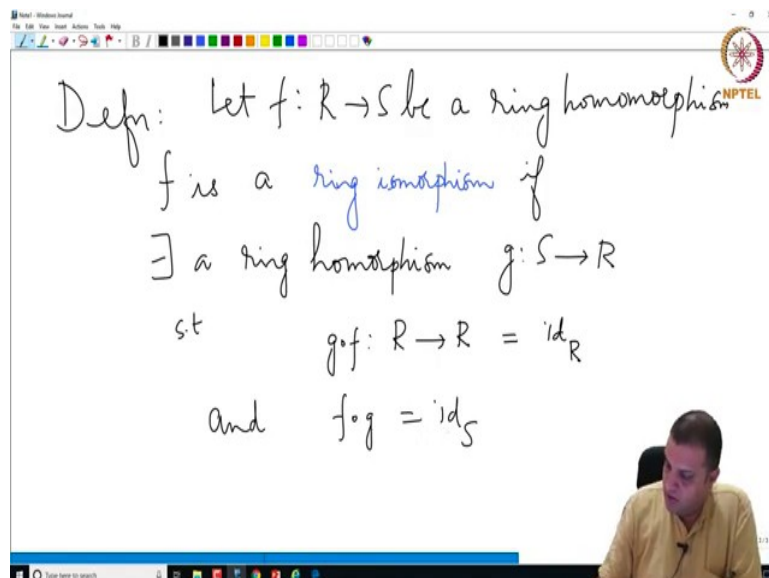


So, let us define a ring homomorphism. So, a ring homomorphism is a function between two rings. So, let R and S be rings. Sorry, before I forget. From now onwards when we say ring, this means commutative ring as we defined last time. We might have to come we might have to deal with some non commutative rings later. But if that is the case, I would explicitly mention that we are discussing a non-commutative ring; otherwise for most of the course, we will only be discussing commutative ring and it is therefore, we will just call it a ring.

So, this is as we defined it last time . So, let R and S be rings and so a function $f: R \rightarrow S$ is a ring homomorphism, if it satisfies the following properties. One, f respects addition; f respects multiplication and these two should be true for every pair of elements $r, r' \in R$ and third, f takes the multiplicative identity of the ring R to the multiplicative identity of the ring S . So, this is what we say, it is a ring homomorphism.

So, remember the first part is said it respects addition, second part is said it respects multiplication and third is said it respects, it takes the additive identity to the additive identity. I am sorry it takes a multiplicative identity to the multiplicative identity, and here; I did put the subscripts to make sure that here we are referring to the one of the ring R and here, we referring to the one of the ring S .

(Refer Slide Time: 03:57)

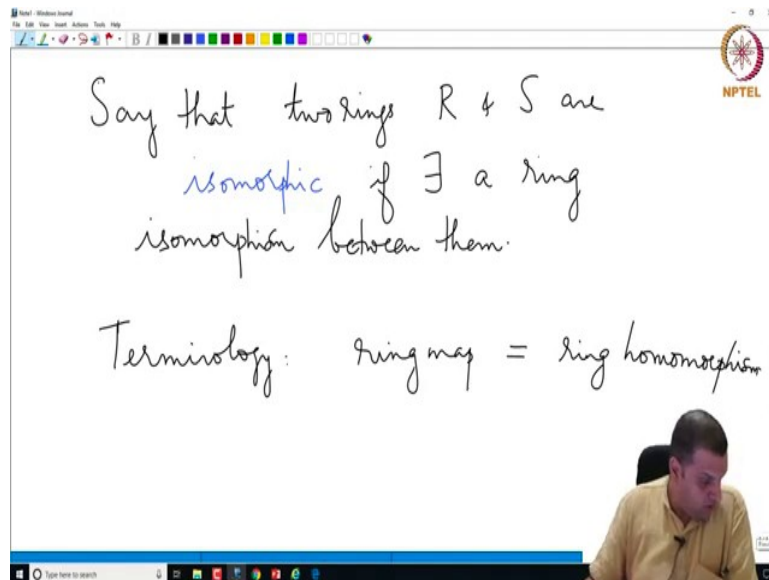


Defn: Let $f: R \rightarrow S$ be a ring homomorphism.
 f is a ring isomorphism if
 \exists a ring homomorphism $g: S \rightarrow R$
 st $g \circ f: R \rightarrow R = \text{id}_R$
 and $f \circ g = \text{id}_S$

Another definition; let $f: R \rightarrow S$ be ring homomorphism; f is said to be an isomorphism, if there exist a ring homomorphism $g: S \rightarrow R$ that is in the opposite direction such that the two composites $g \circ f = \text{Id}_R$ and $f \circ g = \text{Id}_S$.

So, let us look at; so, this is the notation for the map in which f is applied first and then, g is applied. So, this $(g \cdot f)$ is going to be a map from R to R is the identity map on R that is Id_R . And this $(f \cdot g)$ is a map from S to S and this is the identity map on S that is Id_S . The function on R to R given by this composite is identity map and this is the identity map on S .

(Refer Slide Time: 05:45)



Say that two rings R and S are isomorphic, if there exists ring isomorphism between them. So, this is a one does not have to specify in which direction, the isomorphism is because if there is an isomorphism in one direction, the other map is also an isomorphism, so, just one piece of terminology. We might often say ring map to mean a ring homomorphism.

(Refer Slide Time: 07:20)

Exercises : R, S rings, $f: R \rightarrow S$ ring map

(a) $f(0_R) = 0_S$, $f(-r) = -f(r) \forall r \in R$

In fact: $f: (R, +) \rightarrow (S, +)$ is a group homomorphism.

(b) f is an isomorphism $\iff f$ is bijective.

(c) $\exists!$ ring map $\mathbb{Z} \longrightarrow R$:

So, I want to discuss few exercises which I will anyway write up during the course of this, weekly once or twice a week. But let me just at least discuss them. In part because I might use them later without proof, I assuming that you will do these exercises regularly. So, in these exercises R and S will denote rings (commutative rings) and $f: R \rightarrow S$ is a ring map. In other words it is a ring homomorphism. $f(0_R) = 0_S$. So, this is not part of the definition explicitly, but it follows from the definition that this is true.

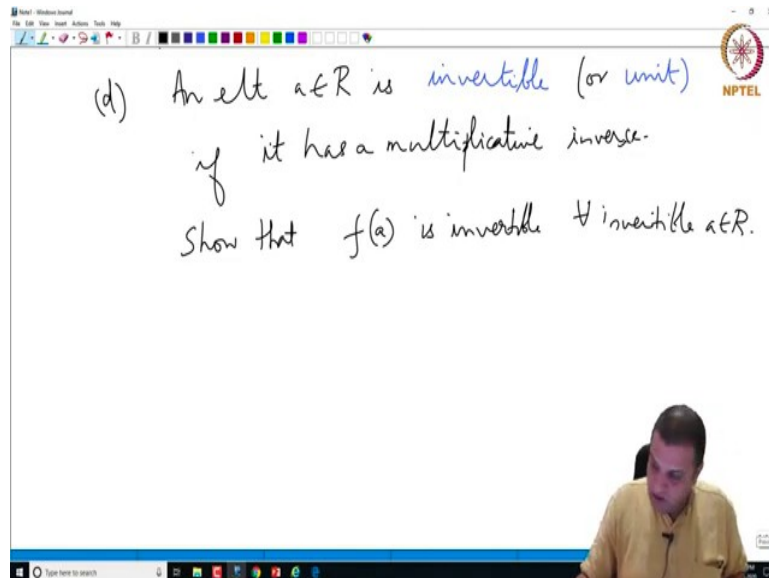
So, one must prove this which is why this was not explicitly stated, the only part that was stated was about the multiplicative identity and $f(-r) = -f(r)$ for all $r \in R$, where minus denotes additive inverse in the two different rings.

So, in fact, I mean putting these together, we see that if you think of it not as a map of rings; but from the Abelian group $(R, +)$ to the Abelian group $(S, +)$ is a group homomorphism. So, in sort, that is the first observation that we would like to make and the second thing that f is an isomorphism, if and only if f is bijective.

So, the point of this exercise is if f is an isomorphism, then there is a g with composites are the two respective identities. So, that will automatically make it a bijective function, but so the contract is in the other direction, that if f is a bijective function; then, the inverse function is a ring homomorphism and then, it has a desired properties and so, please check that. Third exercise, there exists a unique ring map from the set of integers \mathbb{Z} to any ring. Given any ring

R , there is a unique map from the ring of integers \mathbb{Z} . So, this is a unique property of the ring of integers in when we are studying rings.

(Refer Slide Time: 10:17)



So, one more; it is a little definition. An element $a \in R$ is invertible. So, I am defining invertible or sometimes it is called a unit, if it has a multiplicative inverse, we call that in the definition of a ring. We did not say that under multiplication, the nonzero elements form a group; only some elements may have inverses. For example, in \mathbb{Z} , only 1 and -1 have multiplicative inverses. Show that $f(a)$ is invertible, for all invertible $a \in R$; so, just to get familiar with these properties of rings and homomorphisms.

(Refer Slide Time: 11:55)

Polynomial rings

$$R \longrightarrow R[X_1, \dots, X_n]$$

$$r \longmapsto r X_1^0 X_2^0 \dots X_n^0$$

is a ring map.

Prop: Let $f: R \rightarrow S$ be a ring map
and $s_1, \dots, s_n \in S$. Then $\exists!$ ring
map $\tilde{f}: R[X_1, \dots, X_n] \rightarrow S$
st $\tilde{f}(r) = f(r)$
 $\tilde{f}(X_i) = s_i \forall i$

Now, let us look at some examples of these things; polynomial rings. So, then there is a map from $R \rightarrow R[X_1, X_2, \dots, X_n]$, R is a commutative ring in which ring element r goes to the constant polynomial $r X_1^0 X_2^0 \dots X_n^0$. So, this is the ring homomorphism.

So, now this ring homomorphism has a certain universal property and what is that? Let $f: R \rightarrow S$ be a ring map and s_1, s_2, \dots, s_n some elements in S , then there exists a unique ring homomorphism $\tilde{f}: R[X_1, X_2, \dots, X_n] \rightarrow S$, n being the number of elements of s that we chose here to S , such that $\tilde{f}(r) = f(r)$ and $\tilde{f}(X_i) = s_i$ for all $i = 1, 2, \dots, n$.

So, what does it say? It says that given any ring map from R to S and some elements s_1, s_2, \dots, s_n inside S , the ring map extends to a unique ring map from the polynomial ring in n variables over R to S in which the constant polynomials, the constants get mapped as it mapped it, as they were mapped under f and the variables get mapped to the corresponding elements.

(Refer Slide Time: 14:35)

The screenshot shows a whiteboard with the following content:

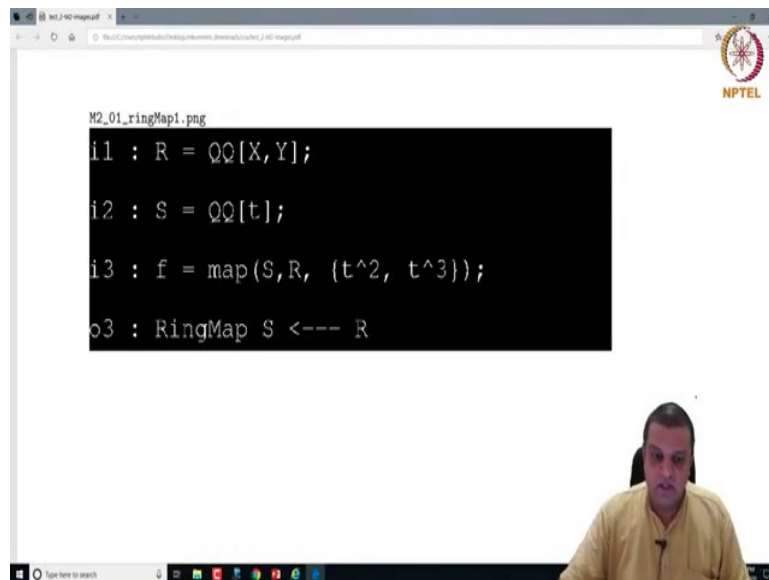
- Handwritten text: Proof: Do the details as an exercise.
- Equation: $\tilde{f}(p(x_1, \dots, x_n)) = f(p)(s_1, \dots, s_n)$
- Text with an arrow pointing to the $f(p)$ term: apply f to the coeffs from R .
- A small box with the text \square (QED).

In the bottom right corner, a lecturer is visible, wearing a yellow shirt. The top right corner of the whiteboard has the NPTEL logo.

So, for proof, you have to show that there exists a map. So, you can just try to do it. So do the details as exercise. I will just define, what I will just give you a hint. And so, if there is a unique map and if you can produce it, it would help us to show what it is. We need to prove its uniqueness. So, define $\tilde{f}(P(X_1, X_2, \dots, X_n))$ of a polynomial $P(X_1, X_2, \dots, X_n)$ to be you first apply f to the constants of P and then, you apply that to s_1, s_2, \dots, s_n .

So, by this, we mean apply f to the coefficients. So, this is the hint and please try to fill in the details and finish this exercise. So, now, let us look at some little bit of Macaulay 2 code to see how this is done in Macaulay 2.

(Refer Slide Time: 16:10)



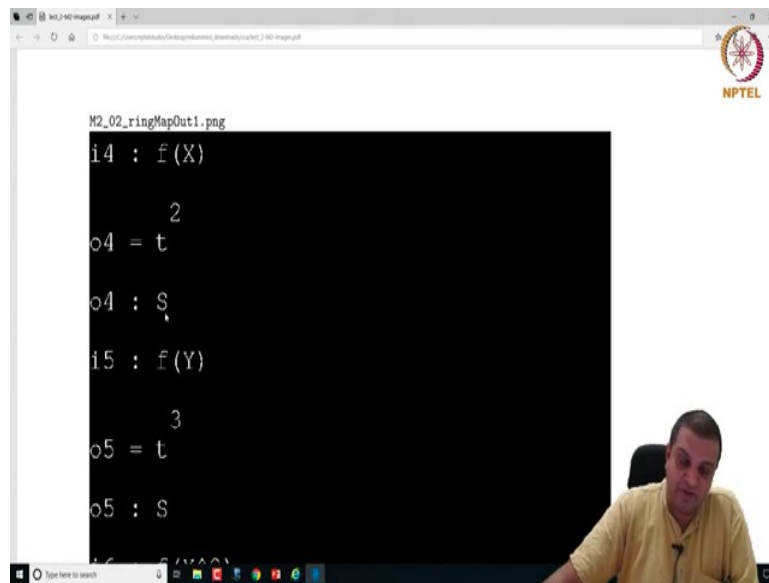
```
M2_01_ringMap1.png  
i1 : R = QQ[X,Y];  
i2 : S = QQ[t];  
i3 : f = map(S,R, {t^2, t^3});  
o3 : RingMap S <--- R
```

So, here is how this is done in Macaulay. So, I am defining a ring with two variables X and Y , with rational coefficients R . Another ring with variable t rational coefficients call that ring S .

Then, we define a map, f , notice the order in which its written. So, typically when we write, we write arrows to the right; but Macaulay the arrow is written to the left and so, it is a ring map from R to S in this from right to left. So, it is written S,R and then, we give a list of elements here.

So things, that are enclosed in these curly brackets. List of elements in here which are what these variables should take. So, this one says that X will go to t^2 and Y will go to t^3 and then, it is understood that rationals will get map identically to the rationals here. So, let us see how let us see if Macaulay has understood, what we asked for it to do.

(Refer Slide Time: 17:23)



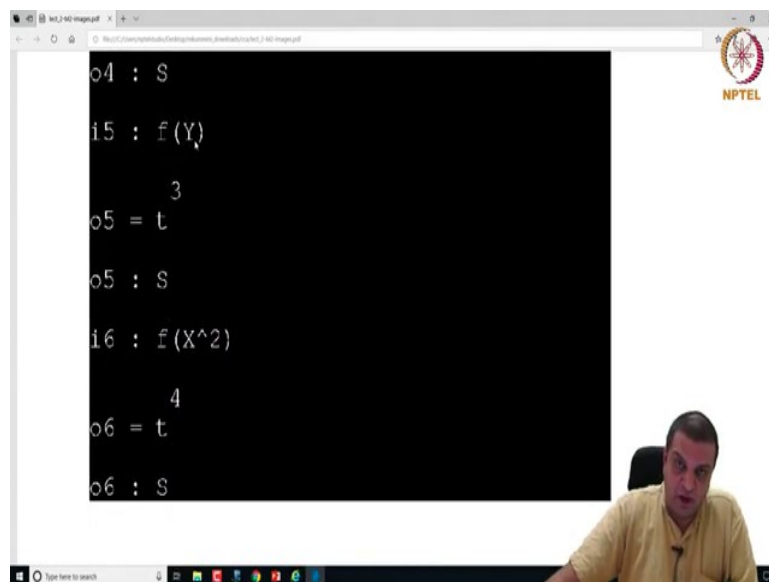
The screenshot shows a Macaulay2 session window with the following text:

```
M2_02_ringMapOut1.png  
i4 : f(X)  
      2  
o4 = t  
      3  
o4 : S  
i5 : f(Y)  
      3  
o5 = t  
      3  
o5 : S
```

A man in a yellow shirt is visible in the bottom right corner of the window.

So, here is the screenshot of the output of we are checking. So, then, we are asking Macaulay what is $f(X)$, then it replies t^2 , element of S .

(Refer Slide Time: 17:35)



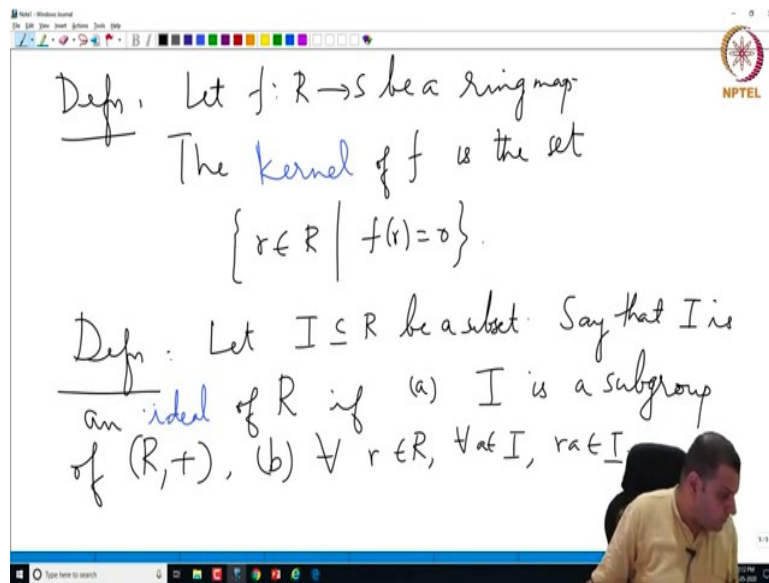
The screenshot shows a Macaulay2 session window with the following text:

```
o4 : S  
i5 : f(Y)  
      3  
o5 = t  
      3  
o5 : S  
i6 : f(X^2)  
      4  
o6 = t  
      4  
o6 : S
```

A man in a yellow shirt is visible in the bottom right corner of the window.

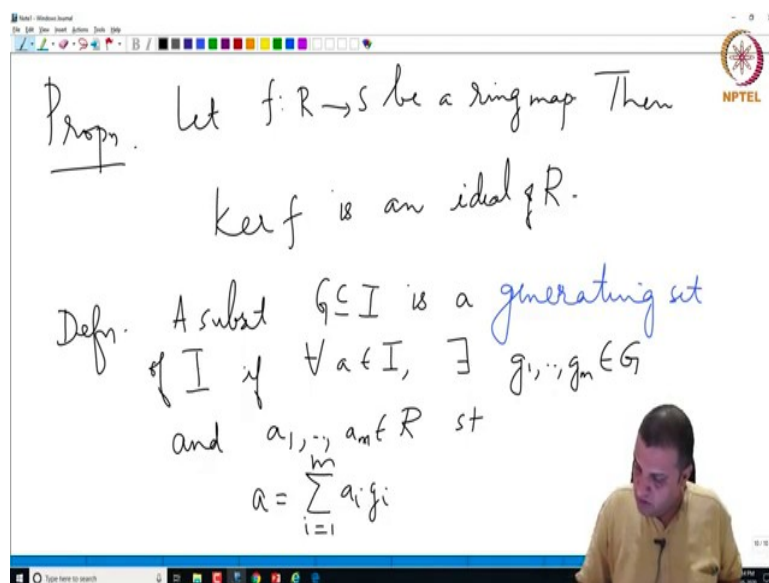
Here, we ask $f(Y)$. In line 5, we ask $f(Y)$., it replies t^3 and an element of S . Then, we ask $f(X^2)$, it is a t^4 , element of S .

(Refer Slide Time: 17:49)



Definition. Let $f: R \rightarrow S$ be a ring map, the kernel of f , is the set $\{r \in R \mid f(r) = 0\}$. Another definition, let I inside R be a subset say that I is an ideal of R , if two conditions; (a) I is a subgroup of the additive group and (b) for all $r \in R$ and for all $a \in I$, ra is inside I . So, it is closed under multiplication by arbitrary elements of the ring and is then, a subgroup of the additive group of R such a thing is called an ideal of R .

(Refer Slide Time: 19:59)



So, here is a proposition which you should prove. Let $f: R \rightarrow S$ be a ring map, then kernel of f is an ideal of R . So, now, we would like to see how Macaulay2 computes these things. So,

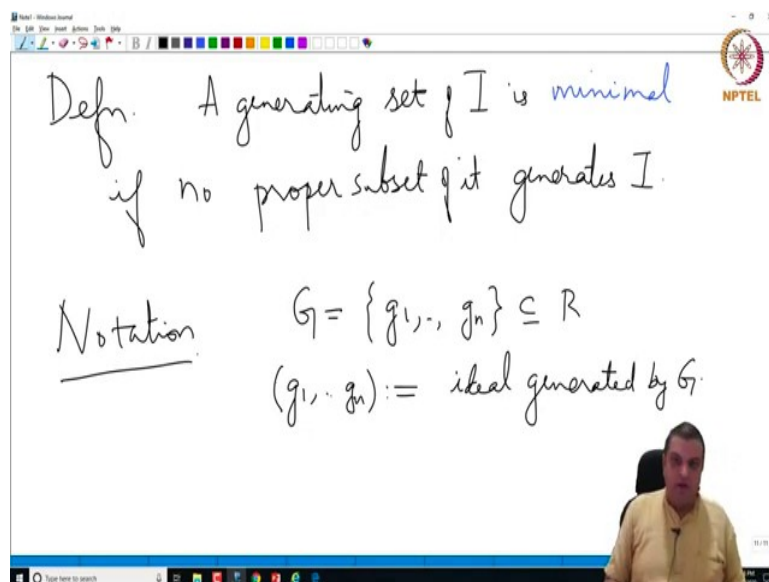
before that, we need to make sense defined just one term. Definition; A subset G inside I is generating set, I is an ideal here.

Sorry, I is an ideal, G is just a subset generating set of I , if for all $a \in I$, there exists a finite

sub collection $g_1, g_2, \dots, g_m \in G$ and $a_1, a_2, \dots, a_m \in R$ such that $a = \sum_{i=1}^m a_i g_i$. That is a is the R

linear combination of these m elements. So, such a set is called a generating set the set itself could be not finite, that we have not just mentioned anyway. However, for every a , we have a finite subset with this property .

(Refer Slide Time: 22:11)

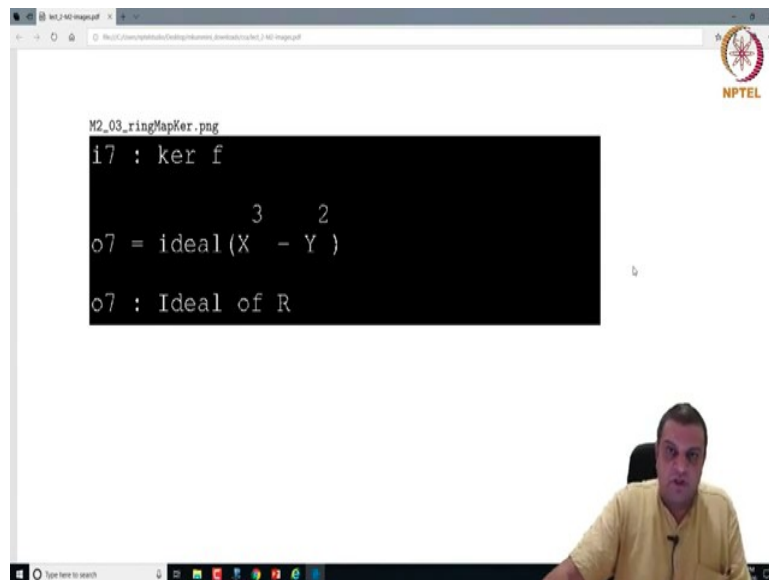


Defn. A generating set of I is *minimal* if no proper subset of it generates I .

Notation $G = \{g_1, \dots, g_n\} \subseteq R$
 $(g_1, \dots, g_n) :=$ ideal generated by G .

A generating set is said to be minimal, if no proper subset of it generates I . So, it is minimal and under containment inclusion of sets . So, just one notation, we will use it mostly for finite sets. So, I will just do it for finite sets, let us say G is a finite set consisting of n elements inside R . Then, we write with ordinary brackets, (g_1, g_2, \dots, g_n) this is the notation for the ideal generated by G .

(Refer Slide Time: 23:42)

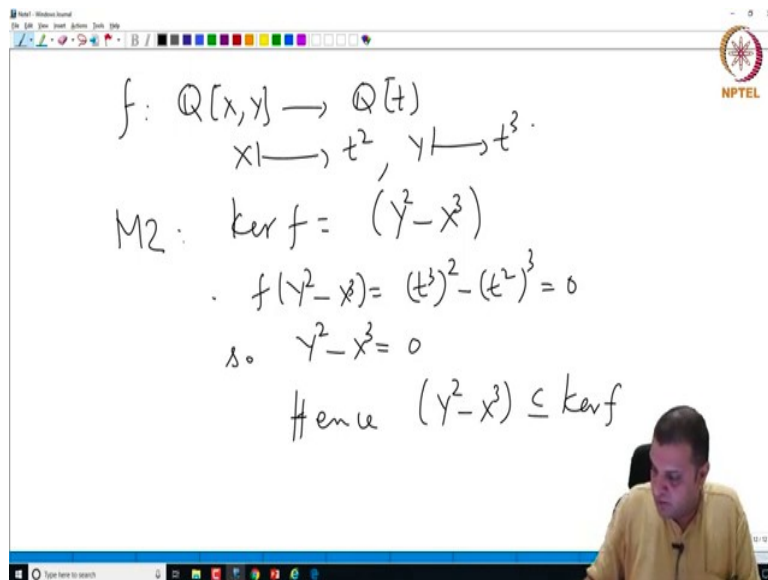


```
M2_03_ringMapKer.prg
i7 : ker f
o7 = ideal (X3 - Y2)
o7 : Ideal of R
```

So, now let us look at an example. So, we asked for kernel of f , remember f is this map which goes from $Q[X, Y] \rightarrow Q[t]$; X goes to t^2 , Y goes to t^3 and we ask for its kernel and it says kernel of f is ideal generated by $X^3 - Y^2$. In other words; every multiple of this polynomial by arbitrary element of R .

So, now we can; so, we do not know how this is computed. As we progress in this course, we will learn how this is computed; how Macaulay2 will compute this. But right now, we will use this as a help for us to prove it, that this is the kernel. So, the details, I will leave as an exercise. I will list out the steps, but let me just briefly say how it is done.

(Refer Slide Time: 25:05)



Handwritten notes on a whiteboard:

$$f: \mathbb{Q}[X, Y] \rightarrow \mathbb{Q}[t]$$

$$X \mapsto t^2, Y \mapsto t^3.$$

M2: $\ker f = (Y^2 - X^3)$

$$f(Y^2 - X^3) = (t^3)^2 - (t^2)^3 = 0$$

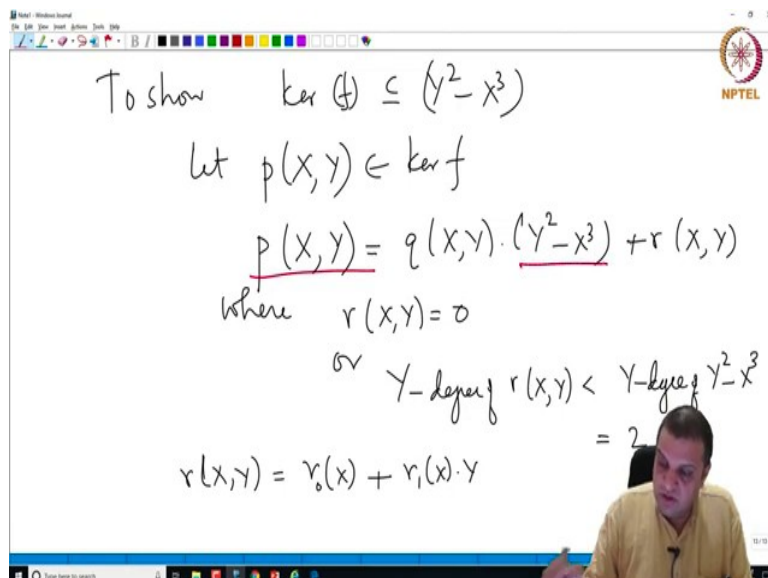
s. $Y^2 - X^3 = 0$

Hence $(Y^2 - X^3) \subseteq \ker f$

So, the map is from $\mathbb{Q}[X, Y] \rightarrow \mathbb{Q}[t]$; X goes to t^2 , Y goes to t^3 and Macaulay2 tells us kernel of f is the ideal generated by $Y^2 - X^3$ and we asked can we prove this statement. So, how do we do this? So, that so first of all we know that. So, now, try to prove this by hand.

We know that $f(Y^2 - X^3) = (t^3)^2 - (t^2)^3 = 0$. Hence $(Y^2 - X^3) \subseteq \ker f$. Now, we want to prove the other inclusion.

(Refer Slide Time: 26:25)



Handwritten notes on a whiteboard:

To show $\ker f \subseteq (Y^2 - X^3)$

Let $p(X, Y) \in \ker f$

$$p(X, Y) = q(X, Y) \cdot (Y^2 - X^3) + r(X, Y)$$

where $r(X, Y) = 0$

or $\deg_Y r(X, Y) < \deg_Y (Y^2 - X^3)$

$$= 2$$

$$r(X, Y) = r_0(X) + r_1(X) \cdot Y$$

So, to show the other inclusion which is $\text{Ker } f \subseteq (Y^2 - X^3)$. So take an arbitrary element here, it is a polynomial in two variables. So now, the point is if you take a polynomial in two variables; one can think of it as a polynomial in the variable Y , where the coefficients themselves are polynomials in X .

One can write this using division algorithm, $p(X, Y) = q(X, Y)(Y^2 - X^3) + r(X, Y)$, all that we have used here is that this is a monic polynomial in the variable Y plus some remainder polynomial X, Y ; where, this has a certain property, either this is 0 or its Y degree should be less than the Y degree of this thing $Y^2 - X^3$ which is 2.

Because, if it had a term that involved Y^2 one could divide by again and then move it to the side. So, in other words $r(X, Y)$ is of the form $r_0(X) + r_1(X)Y$ and one has to show that. So, the point is that $p(X, Y)$ is in the kernel of f , this is in the kernel, this is in the kernel, this is in the kernel. So, both p and this term at the kernel, so; the term on the left and the first term on the right are in the kernel.

(Refer Slide Time: 28:36)

Hence $f(r_0(X) + r_1(X)Y) = 0$

$$\Rightarrow \underbrace{r_0(t^2)}_{\text{even deg in } t} + \underbrace{r_1(t^2)t^3}_{\text{odd deg in } t} = 0$$

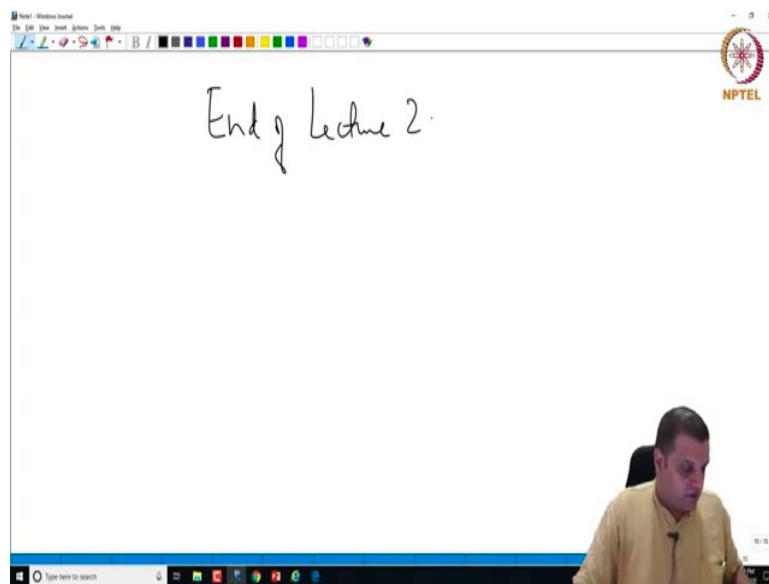
$$\Rightarrow r(X, Y) = 0$$

$$\Rightarrow p(X, Y) \in (Y^2 - X^3)$$

So, hence, $f(r_0(X) + r_1(X)Y) = 0$ and this will so what does that say? This says $r_0(t^2) + r_1(t^2)t^3 = 0$. Now, I will just say what this is. So, this is a polynomial in t in which every term has even degree. This whole thing, while this is odd, the entire thing after multiplying by t cubed is odd degree in t and the way they can be 0.

The sum can be 0, only if both of them are 0 and that says that which says that $p(X, Y)$ is in the kernel of f . So, there are some exercises, one if you have not seen a proof of the division algorithm for rings like this, then please for monic polynomials, please learn that and then, check these details. So, this is the proof. So, this is how we use these computational algebra systems many times which is it shows us a computation and tells us what we can prove and perhaps even how we should go about proving it.

(Refer Slide Time: 30:26)



So this is the end of a 2nd lecture. In the next lecture, we will look at prime ideals, maximal ideals, operations on ideals and then, we will prove what is Noetherian rings and we will prove. So, in the next few lectures, we will prove what is called the Hilbert Basis Theorem; simultaneously, developing some ideas of computation.