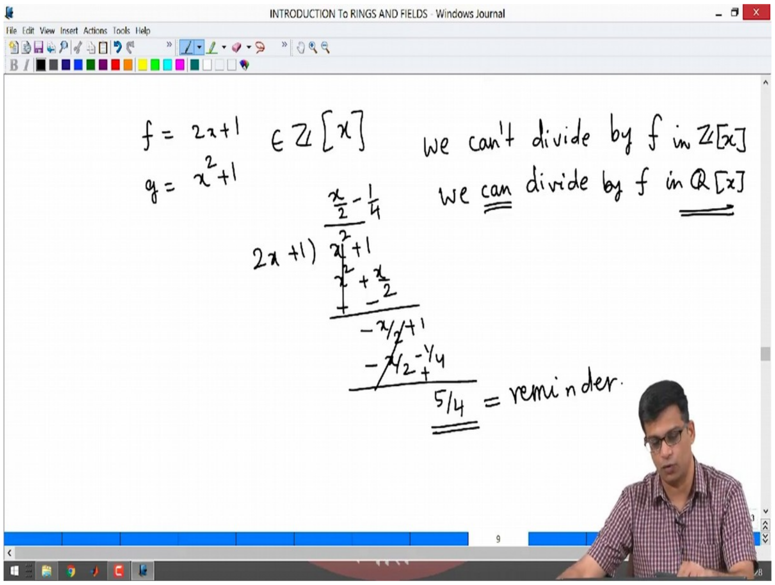
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 05
Polynomial rings 2

So, ok, let us continue now with division inside the polynomial ring. So, as an example, I did in the last video shows we can divide as long as the polynomial has leading coefficient 1. So, just to give you an idea of what the problem will be, let us consider the following example.

(Refer Slide Time: 00:35)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$f = 2x+1 \quad \in \mathbb{Z}[x]$

$g = x^2+1$

We can't divide by f in $\mathbb{Z}[x]$

We $\underline{\underline{can}}$ divide by f in $\underline{\underline{\mathbb{Q}[x]}}$

$$\begin{array}{rl} & \frac{x}{2} - \frac{1}{4} \\ \hline 2x+1) & \cancel{x^2} + 1 \\ & \overset{-}{\cancel{x^2}} \overset{-}{+} \frac{x}{2} \\ \hline & -\cancel{x/2} + 1 \\ & \overset{+}{-}\cancel{x/2} \overset{+}{-} 1/4 \\ \hline & \underline{\underline{5/4}} = \text{reminder.} \end{array}$$

Let us take f to be 2 x plus 1 and g to be x square plus 1. So, they are both inside, let say the polynomial ring over the integers. So now, we cannot divide by f. Why not? Because let us say you want to do the procedure that I did in the previous video.

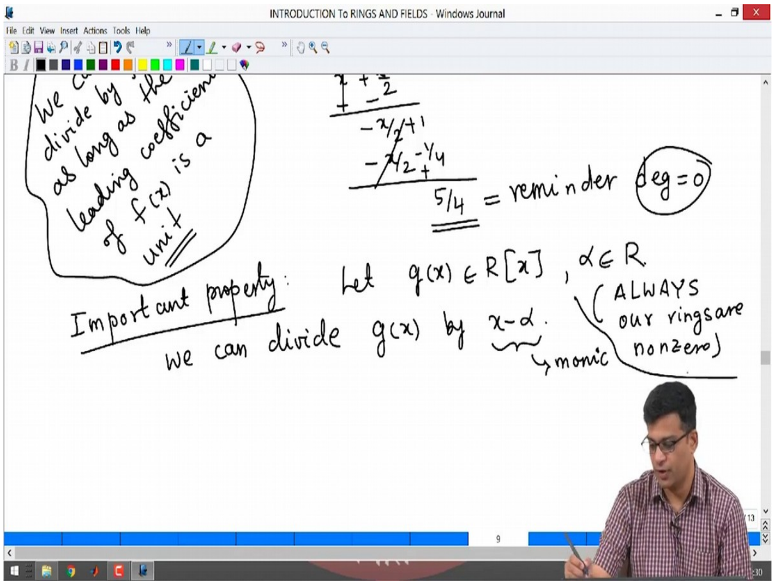
So, you will start with this, but now in order to get x squared from 2 x, you will have to somehow cancel 2, but there is no way that you can do it in the integers. So, you cannot put anything here to get x squared here in order to cancel. So, you cannot divide by f, the correct sentences in the polynomial ring Z[x].

However, I claim we can divide by f in Q[x] because we can get x squared here. Why is that? Because 2x when you multiply by 1 by 2 or x by 2 gives me x squared. So now, this existence of 1 by 2 is what makes this work, which exists in Q, but not in Z. So, we can divide by f in Q[x]. So, and what do we get 2 x plus 1.

So, you get x by 2, then you get will be x squared here and it will be x by 2 here. So, now, if you subtract, this will go away this will be minus x by 2 plus 1. Now, to get minus x by 2, what you will do is plus 1 by 4 right or minus 1 by 4 really. Because you want to get minus x by 2; so, minus 1 by 4 times 2 x is minus x by 2; minus 1 by 4 times 1 is minus 1 by 4.

And you get so, it is x squared minus 1 I am taking. So, let me change that. So, yeah so, it does not matter. So, it will be 1 by 4 plus 1. So, this is 5 by 4 right. So, this is the remainder and remember, remainder should have degree strictly less than the degree of 2 x plus 1. In this case, it is correct.

(Refer Slide Time: 03:05)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

We c divide by as long as the leading coefficien of $f(x)$ is a unit

$$\begin{array}{l} -\frac{x}{2}+1 \\ -\frac{x}{2}-\frac{1}{4} \\ \hline \frac{5}{4} = \text{reminder} \quad \boxed{deg=0} \end{array}$$

Important property: Let $g(x) \in R[x]$, $\alpha \in R$

we can divide $g(x)$ by $\underbrace{x-\alpha}_{\hookrightarrow \text{monic}}$.

(ALWAYS our rings are nonzero)

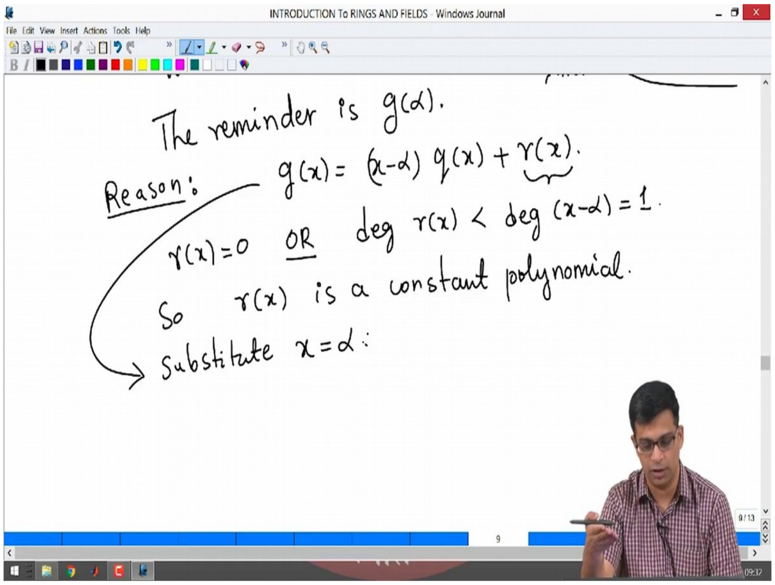
So, degree is 0, correct. So, we can divide in Q[x] so. In fact, the statement should be that we can divide by f as long as the leading coefficient of f is a unit. I described in the last video that leading coefficient has to be 1, but really it is not necessary that it is 1. The reason that 1 works is because 1 is a unit. So, that you can first get rid of these terms here ok; these terms here can be gotten rid off.

So, it is not just when leading coefficient is 1 that you can divide, you can divide as soon as leading coefficient is a unit. In the polynomial in Q[x], the leading coefficient of 2 x plus 1 which is 2 is a unit. In the polynomial ring Z[x], the leading coefficient of 2 x plus 1 which is 2 is not a unit.

So, you cannot divide in Z[x] and I want to write one more important property that is useful to keep in mind and this example illustrates this. Suppose, so important property. So, let say g x is an element of a polynomial ring and let alpha be an element of R. So, we can divide g x by we can divide right because x minus alpha has leading coefficient 1 and this is monic.

So, in any ring we can divide. So, I will always assume remember our rings are nonzero. So, we will assume our rings are nonzero. So, 1 is different from 0 in that ring. So, this is a monic polynomial. So, we can divide g x by x minus alpha.

(Refer Slide Time: 05:31)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
9/13
9
09:12

The reminder is $g(\alpha)$.

Reason: $g(x) = (x-\alpha)\, q(x) + r(x)$.

$r(x) = 0$ OR $\deg r(x) < \deg (x-\alpha) = 1$.

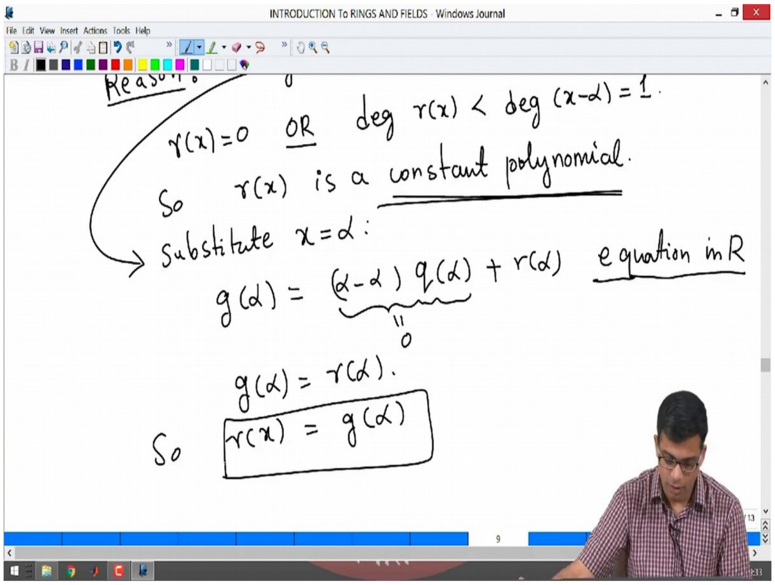
So $r(x)$ is a constant polynomial.

Substitute $x = \alpha$:

Then, the remainder I claim is simply g of alpha. Why is that? The reason for this is the following. So, reason so, remember when you divide g x by x minus alpha, you will have some q x here plus some reminder right. The remainder should have degree. So, and we know what are the properties of the reminder. Reminder is either 0 or degree of the reminder is less than the degree of x minus alpha which is 1.

So, in other words, the degree of r x is strictly less than 1 or r x is 0; either way r x is a constant polynomial right. Because we are dividing by a degree 1 polynomial x minus alpha, the reminder should be a constant polynomial. Now, let us look at this equation g x equals x minus alpha q x plus r x and substitute x equal to alpha. This is an important operation. So, if you have a polynomial identity, if you replace x by a specific element of the ring; you get an equation in the ring.

(Refer Slide Time: 07:03)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

Reason:

$r(x)=0$ OR $\deg r(x) < \deg(x-\alpha) = 1$.

So $r(x)$ is a constant polynomial.

Substitute $x=\alpha$:

$$g(\alpha) = \underbrace{(\alpha-\alpha)\,q(\alpha)}_{0} + r(\alpha)$$ equation in R

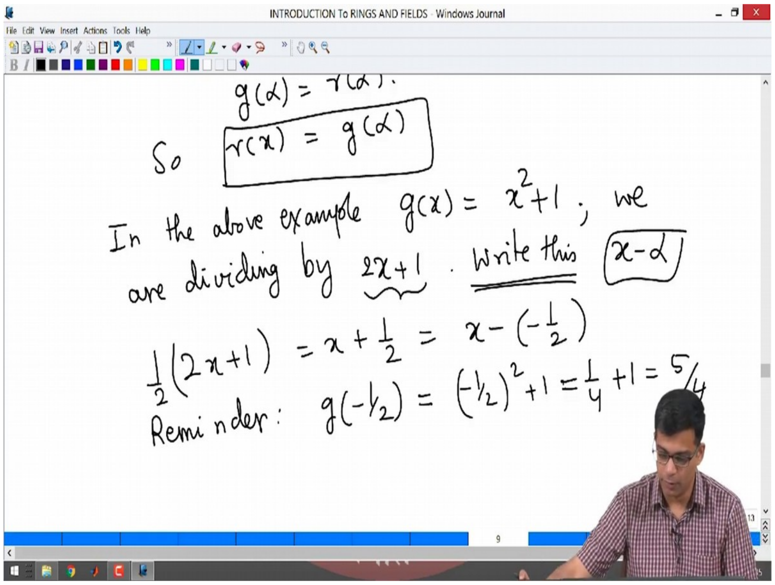
$$g(\alpha) = r(\alpha).$$

So $\boxed{r(x) = g(\alpha)}$

So, if you substitute x equal to alpha, you get g alpha on the left hand side; alpha minus alpha times q alpha plus r alpha. So now, this is an equation in R. Now, x is gotten rid of right. So, x is gone, what you are left with is actually an equation in R. But now alpha minus alpha is 0. So, this whole thing is 0. So, g alpha is r alpha. But note that we have already noticed that r x is a constant polynomial and g alpha is r alpha. So, r x must be just g alpha because we have a constant polynomial it does not depend on x and at alpha, it is r alpha means it is g alpha.

So, this tells me that when I divide by a linear polynomial x minus alpha, the reminder is simply the value of the polynomial when you evaluate x equal to alpha and if you go back to this example that I did in the beginning of today’s video here I am doing x squared.

(Refer Slide Time: 08:15)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$g(\alpha) = r(\alpha).$

So $\boxed{r(x) = g(\alpha)}$

In the above example $g(x) = x^2+1$; we are dividing by $\underset{\sim}{2x+1}$. $\underline{\text{Write this}}$ $\boxed{x-\alpha}$

$\frac{1}{2}(2x+1) = x+\frac{1}{2} = x-\left(-\frac{1}{2}\right)$

Remi nder: $g(-1/2) = (-1/2)^2+1 = \frac{1}{4}+1 = 5/4$

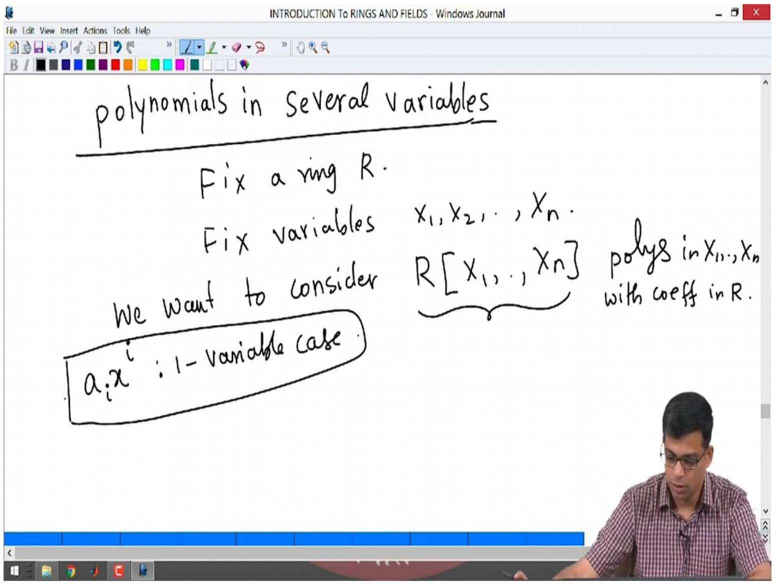
In the above example, in the above example g x is x squared plus 1 and we are dividing by; we are dividing by x minus or rather we are dividing by 2 x plus 1. Now, we need to write this in terms write this like x minus alpha. So, I cannot quite write this, it is not of the form x minus alpha, but we can multiply this by a unit. So, 2 x plus 1 times 1 by 2 becomes x plus 1 by 2 which can be written as x minus minus 1 by 2. So, the important point when you are dealing with division in polynomial rings is you can always multiply the polynomial by a constant; reminder does not change.

So, here division by 2 x plus 1 is really division by x plus 1 by 2 which is x minus minus 1 by 2. So, the reminder by the property that I wrote earlier should be g of minus 1 by 2 right. g of minus 1 by 2 is minus 1 by 2 squared plus 1 which is 1 by 4 plus 1 which is 5 by 4 and remember this is exactly the remainder that we got, right. The remainder is simply evaluating the polynomial at minus 1 by 2.

So, this is always true, when you are dividing by a polynomial of the form x minus alpha, what you get is simply g of alpha ok. So, this is useful to keep in mind. The next, so this is our discussion about polynomial ring in 1 variable because I want to introduce now polynomial rings in several variables.

But just to recap what we have done, we have introduced polynomials in a single variable x; x is really a symbol. Its expressions in as powers of x with the coefficient coming from R in front of it and then, we learnt how to add them; we learnt how to multiply them and we observed that it becomes a ring. Next, we learnt how to divide polynomials; while division is not always possible. We can always divide as long as the leading coefficient is 1 or unit more generally.

(Refer Slide Time: 11:01)



polynomials in several variables

Fix a ring R.

Fix variables $X_1, X_2, \ldots, X_n$.

We want to consider $\underbrace{R[X_1, \ldots, X_n]}$ polys in $X_1, \ldots, X_n$ with coeff in R.

$\boxed{a_i x^i : 1\text{- variable case}}$

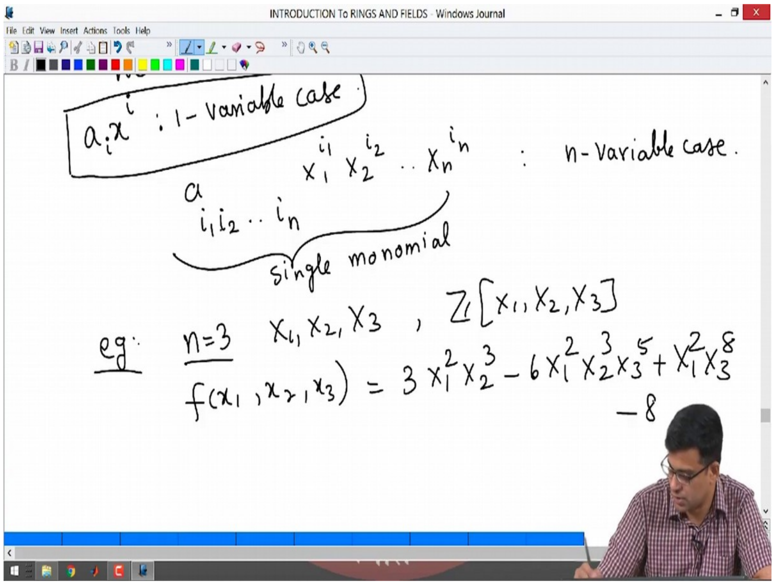
INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

So, now, we want to talk quickly about polynomials in several variables ok. So, this is a we will not discuss a lot at this point because this will come up later for us and at that time I will say more. But at this point I will just want to quickly tell you what I mean. So, several variables means more than 1 variable.

So, we will again fix a ring R and now we fix variables or symbols let us say n of them X 1, X 2 X n and we want to consider R square bracket X 1 up to X n. Earlier we had R square bracket a single variable X and now we have n variables. So, these are going to be polynomials in X 1 through X n with coefficients in R ok.

So, just like in the earlier case when you had monomials of this form right, we have monomials of this form in the 1 variable case. What we will now have is in; so, here we will have let say I will not write n because I have used it here. So, this is 1 variable case. If you remember a polynomial is made up of terms like this we add several of them together. Here, multivariable polynomial will be made up of terms like this.

(Refer Slide Time: 13:01)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$\boxed{a_i x^i : \text{1-variable case.}}$

$\underbrace{a_{i_1 i_2 \dots i_n} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}}_{\text{single monomial}}$: n-variable case.

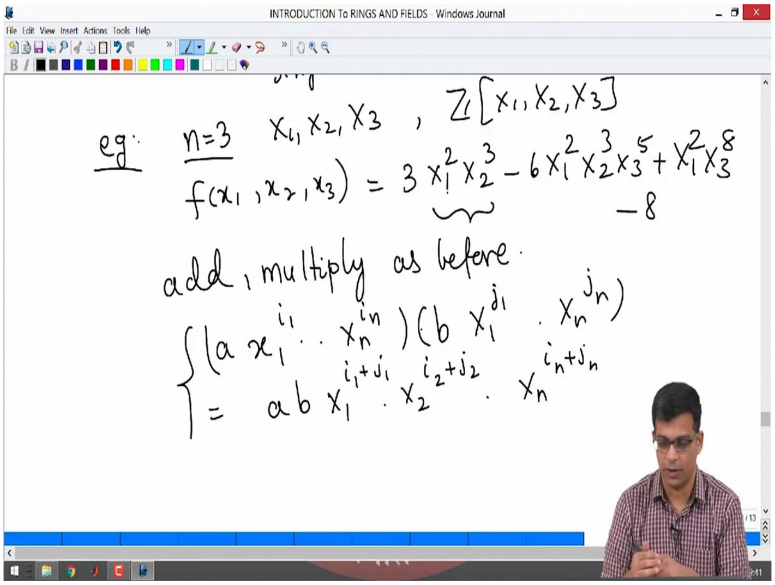
eg: $n=3$ X_1, X_2, X_3 , $\mathbb{Z}[X_1, X_2, X_3]$

$f(x_1, x_2, x_3) = 3X_1^2X_2^3 - 6X_1^2X_2^3X_3^5 + X_1^2X_3^8 - 8$

So, we will have a i 1 i 2 i n. So, this will be a subscript ok. These n indices and we will have the variables will be X 1 i 1 X 2 i 2 X n i n. So, this is the n invariable case ok. So, in n variables, these are the monomials. So, this is a single monomial ok. Now, a polynomial will simply be a several of these added together.

So, as an example let us take n is 3. So, you have X 1, X 2, X 3; what is the polynomial? So, here we will write f 1 f of x 1 and let say I am looking at Z X 1, X 2, X 3. So, f x 1, x 2, x 3 will be example of such a polynomial will be let us say 3 X 1 squared X 2 cubed minus 6 X 1 squared X 2 cubed X 3 5 plus X 1 squared X 3 over 8 minus 8. I am just randomly writing something. So, several such things together so, now each monomial as a degree attached to this is like 2 3 0.

(Refer Slide Time: 14:37)



INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

eg: $\underline{n=3}$ X_1, X_2, X_3 , $\mathbb{Z}[X_1, X_2, X_3]$

$$f(x_1, x_2, x_3) = 3\underbrace{X_1^2 X_2^3} - 6X_1^2 X_2^3 X_3^5 + X_1^2 X_3^8 - 8$$

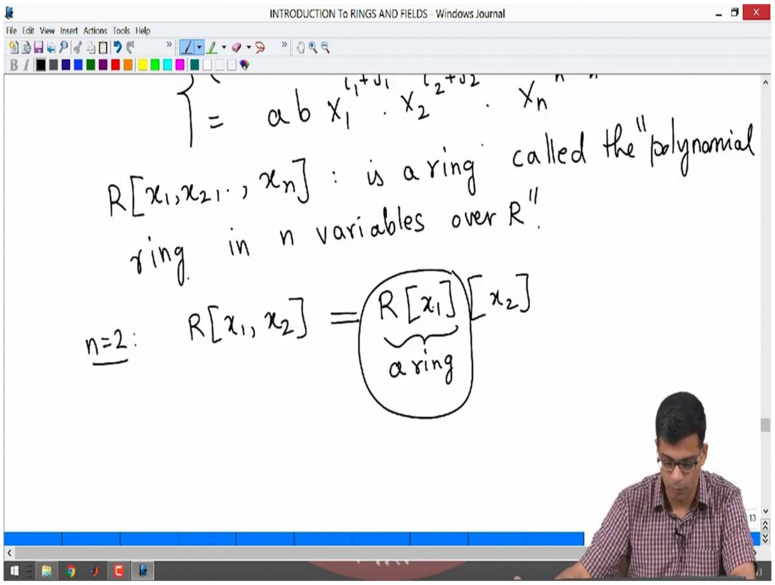
add, multiply as before.

$$\begin{cases} (a\, x_1^{i_1} \cdots X_n^{i_n})(b\, X_1^{j_1} \cdot X_n^{j_n}) \\ = ab\, X_1^{i_1+j_1} \cdot X_2^{i_2+j_2} \cdot X_n^{i_n+j_n} \end{cases}$$

So, it is a triple; this will be 2 3 5, this will 2 0 8, this is 0 0 0. So, now, we can add and multiply as before. It is exactly the same process as before slightly more complicated looking because now we have to keep track of degrees as tuples. So, if you add 2 polynomials in 3 variables you have to compare like terms. So, like term will be things which have X 1 squared X 2 cubed. In the other polynomial, you will see if there is such a term and then, you compare you add the co-efficients. Multiplication is the same. How do you multiply again, I have to do only tell you how to multiply 2 monomials.

So, let us say we have this and this; how to multiply them? I will simply multiply the coefficients because they are elements of R and exponents I will add just like before. So, i 1 plus j 1 X 2 power i 2 plus j 2 all the way to X n power i n plus j n ok. So, this is multiplying a single monomial with another single monomial. Now, how to multiply arbitrary monomials? You will simply one by one, you multiply; just like you did in the case of single variable polynomials. So, this is just to give you an idea of how to multiply and add 2 multivariable polynomials.

(Refer Slide Time: 16:35)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$$\} = a b \, x_1^{i_1+j_1} \cdot x_2^{i_2+j_2} \cdot \; x_n$$

$R[x_1, x_2, .., x_n]$: is a ring called the "polynomial ring in n variables over R".

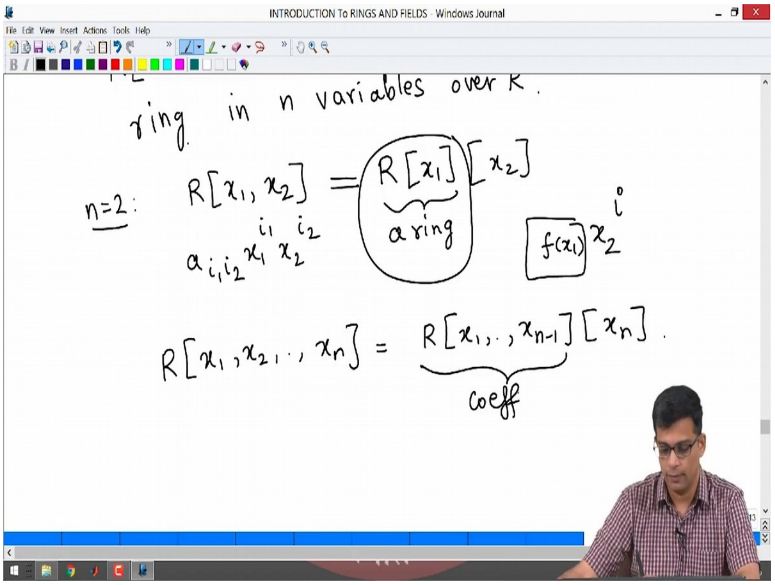
$$n=2: \quad R[x_1, x_2] = \boxed{\underbrace{R[x_1]}_{\text{a ring}}}[x_2]$$

So, now one final comment about this; just like we can we have not verified that, but it is an easy fact to verify. Single variable polynomials form a ring here also R x 1 ok. So, this is a polynomial ring. So, this is a ring rather I should say first. So, polynomials in n variables with the addition and multiplication that, I briefly described is a ring called the "polynomial ring in n variables over R".

So, earlier we talked about one variable polynomial ring. So now, we have a polynomial ring in n variables over R and one easy way to think of this for example, let say 2 variable polynomial ring, I want to consider. So, R x 1, x 2 so, these are polynomials in x 1 and x 2 with coefficients in R. I want you to convince yourself that this is actually nothing but R adjoined x 1 first. So, this is a ring right this we discussed earlier and then, you do x 2.

Because we have talked about polynomial rings over any ring, I will I can take this ring and consider polynomials over this ring in one variable. The new variable I will call x 2 because x 1 is already used. There is no difference between these two things. Here, the terms are sums of this kind right. So, a i 1 i 2 x 1 i 1 x 2 i 2.

(Refer Slide Time: 18:23)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

ring in n variables over R.

n=2: $R[x_1, x_2] = \underbrace{R[x_1]}_{\text{a ring}}[x_2]$

$a_{i_1 i_2} x_1^{i_1} x_2^{i_2}$

$\boxed{f(x_1)} x_2^{i}$

$R[x_1, x_2, \ldots, x_n] = \underbrace{R[x_1, \ldots, x_{n-1}]}_{\text{coeff}}[x_n]$.

So, you take a monomial like this and you add several of these together to get an element of this. What would be things here? Things here will be x 2 power i, but the coefficient would be a polynomial in this right. So now, if you break a f x 1 as a sum of monomials in x 1 and multiply by x 2 i, you will get this. So, they are really looking at the same thing in two different ways and the advantage of thinking it in these terms is this is a process that you already understand. Because earlier we have discussed given a ring R, how to construct a polynomial ring in 1 variable and that is exactly what I have done here ok.

So, in order to understand polynomial ring in 2 variables, all you need to understand is polynomial ring in 1 variable over polynomial ring in 1 variable. So, similarly if you want to understand what is x 1, x 2, x n, polynomial ring in n variables, this is nothing but you first consider the polynomial ring in n minus 1 variables and you add 1 variable ok. So, this is just adding a polynomials in a single variable called x n with coefficients coming from x polynomial ring in n minus 1 variables.

So, this is our coefficients ok. So, and again as I said these are exactly the same objects, but our view is different; our perspective is different and we will not initially at least discuss much about polynomial rings in several variables. But, I wanted to discuss at least define them. So, that you are familiar with it.

I am going to end this video here. In the next video, we will continue with our study of rings and will study homomorphism and ideals and so on.

Thank you.