

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

**Lecture – 07**  
**Division Algorithm**

(Refer Slide Time: 00:27)

Division algorithm for  
multivariate polynomials

$K$  field

Single variable

$R = K[x]$

$f, g \in R, \quad g \neq 0$

NPTEL

This is the 7th lecture in this course. So, the idea for this, the topic for this course is to understand what is called Division Algorithm; division algorithm for multivariate polynomials. So, let us look at what we know. So, in one variable, suppose  $R$  is  $K[x]$ . So, again keep throughout these things  $K$  is a field; and let us say  $f, g \in R$  and  $g$  is non-zero.

(Refer Slide Time: 01:36)

$$\begin{aligned} \exists q, r \in R \text{ st} \\ f = q \cdot g + r \\ \text{where } r = 0 \\ \text{or } \deg r < \deg g \end{aligned}$$



So, then what does the division algorithm say? There exist  $q, r \in R$ , such that  $f = qg + r$ , where  $r = 0$  or  $\deg(r) < \deg(g)$ .

So, this is the most basic version that we know, we just divide  $f$  by  $g$  and then prove that this is true. But how do we see this, because we would like to generalize such a statement to larger number of variables and possibly larger number of  $g$ 's also. But, how do we see in this, in this new language of term orders?

(Refer Slide Time: 02:25)

Note that  $\exists!$  monomial order  
on  $R$   
 $1 < x < x^2 < \dots$   
"  $r = 0$  or  $\deg r < \deg g$  "  
"  $r = 0$  or  $\text{in}_> g \nmid \text{any term of } r$  "

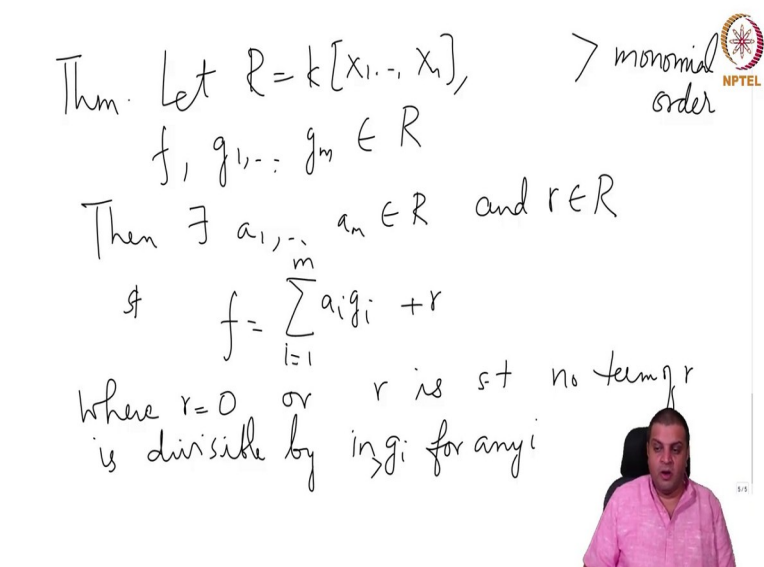


So, note that there is a unique monomial order  $R$  which is  $1 < x < x^2 < \dots$ .

We already noticed that, if one monomial divides another monomial, the one the smaller one is lower in the order. So, there is only one order this way. And then what we are saying is that  $r = 0$  or  $\deg(r) < \deg(g)$ . So, this is the condition on  $r$  is the same as  $r = 0$  or the  $\text{in}(g)$  does not divide any term of  $r$ .

Then it really gets reinterpreting that in terms of initial terms, leading terms; that is because the degree is less than this initial term is  $x$  to this degree, where all of these things that are smaller degree, all the terms here are smaller degree. So, this is the statement for one variable; this has been, we have already used one version of it in multivariate, where we have one new variable and the monic polynomial. So, that is not exactly the generalization that we want or we looking for.

(Refer Slide Time: 04:19)



Thm. Let  $R = k[x_1, \dots, x_n]$ ,  $f, g_1, \dots, g_m \in R$

Then  $\exists a_1, \dots, a_m \in R$  and  $r \in R$

$\& \quad f = \sum_{i=1}^m a_i g_i + r$

where  $r = 0$  or  $r$  is s.t. no term  $r$  is divisible by  $\text{in} g_i$  for any  $i$

$>$  monomial order

NPTEL

So, here is a theorem that we will prove now. Let  $R = k[X_1, \dots, X_n]$ ;  $f, g_1, \dots, g_m \in R$ , we want to divide  $f$  by these, the whole family, not just by a single. Then there exist

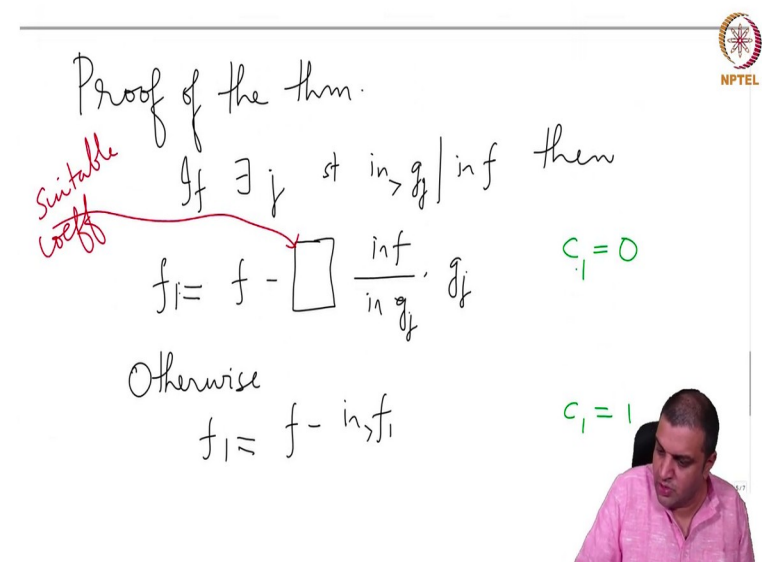
$$a_1, \dots, a_m \in R \text{ and } r \in R, \text{ such that } f = \sum_{i=1}^m a_i g_i + r$$

Now, again what is the condition of  $r$ ? it is exactly as the one that we stated earlier, where  $r = 0$  or  $r$  is such that no term of  $r$  is divisible by  $\text{in}(g_i)$ . So, again there is some underlying monomial order on  $\mathcal{G}$  for any  $i$ . So, this is the division algorithm or division theorem for multivariate polynomials. So, this is always with respect to a given monomial order.

The basic case was also with respect to a given monomial order; it is just set using implicit and we never thought of it as monomial order, but the principle is the same. So, how do we prove this? The proof is a little algorithmic. it is a little informal maybe. So, I have I have tried to explain the algorithm and then you will see an example in macaulay2, where we work from the algorithm.

And from there you would understand. So, if you look at the book of Cox, Little and O'shea, then there is a formal way of looking at the algorithms written and its termination and characteristic proof. So, we will do it some one of the formula. Let us ask, let us do the following. So, we asked this. So, proof is we will construct some elements and then we will prove that this is enough. So, proof is here.

(Refer Slide Time: 07:18)



Proof of the thm.

*Suitable choice*  $\exists j \text{ st } \text{in}(g_j) \mid \text{in}(f) \text{ then}$

$$f_1 = f - \left[ \frac{\text{in}(f)}{\text{in}(g_j)} \right] g_j \quad c_1 = 0$$

Otherwise

$$f_1 = f - \text{in}(f) \quad c_1 = 1$$

So, at every stage we ask the following question. So, this is the starting stage; if there exist  $j$  such that initial term of  $\text{in}(g_j)$  divides  $\text{in}(f)$  then, We just remove the initial

term; the  $f_1 = f - \dots \frac{in(f)}{in(g_j)} g_j$  So, a suitable coefficient here, so I will just write a box here; because this to be suitable coefficient.

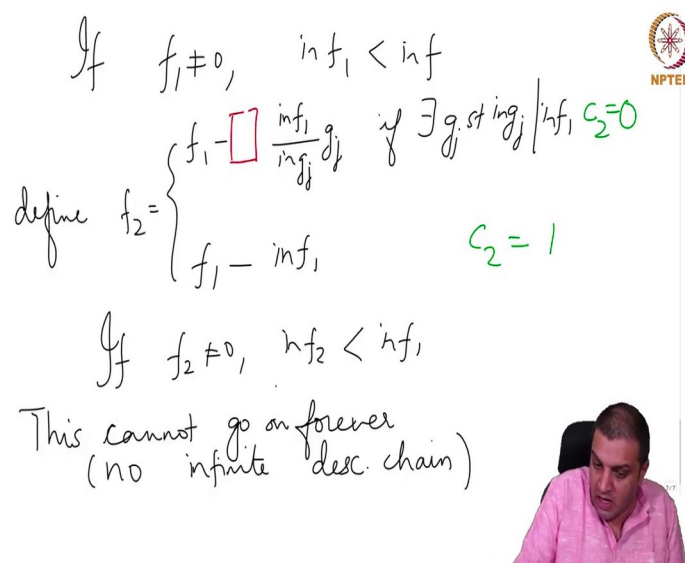
So, again you repeat the suitable coefficient here is put in, so that the leading term coefficients are canceled there and the leading term is removed from this.

So, this is what we did. Otherwise, define  $f_1 = f - in(f_1)$ ; there is no  $j$  here just. So, this is the step that we will do at every stage and we would need when we come back later we would need to keep track of what was the step that at every stages.

So, we will write for this one, we will write  $c_1 = 0$ . In this proof, we just have to keep track what was the operation that was done at every stage; was it canceling the leading coefficient by suitably multiply with  $g_j$  or was it just subtracting the leading term? So, this has to be kept track when we were come back to finish the proof. So, we will denote this thing that, we removed we cancel the leading term by a suitable  $g_j$  that statement we will keep track by writing  $c_1 = 0$  and this one we will denote by  $c_1 = 1$ .

So, there is no significance for the numeric value 0 or 1, which is just a binary value; one has to just keep track of what would we do to go from  $f$  to  $f_1$ . So, now, let us observe this thing.

(Refer Slide Time: 10:35)



$$\text{If } f_1 \neq 0, \quad \text{in } f_1 < \text{in } f$$

$$\text{define } f_2 = \begin{cases} f_1 - \frac{\text{in } f_1}{\text{in } g_j} g_j & \text{if } \exists g_j \text{ s.t. } \text{in } g_j \mid \text{in } f_1, c_2 = 0 \\ f_1 - \text{in } f_1 & c_2 = 1 \end{cases}$$

$$\text{If } f_2 \neq 0, \quad \text{in } f_2 < \text{in } f_1$$

This cannot go on forever  
(no infinite desc. chain)

If  $f_1 \neq 0$ , then what we just did was to remove the leading term and therefore,  $\text{in}(f_1) < \text{in}(f)$ ; in either one of those steps, the  $f_i$ 's leading term is strictly smaller than the leading term of  $f$ .

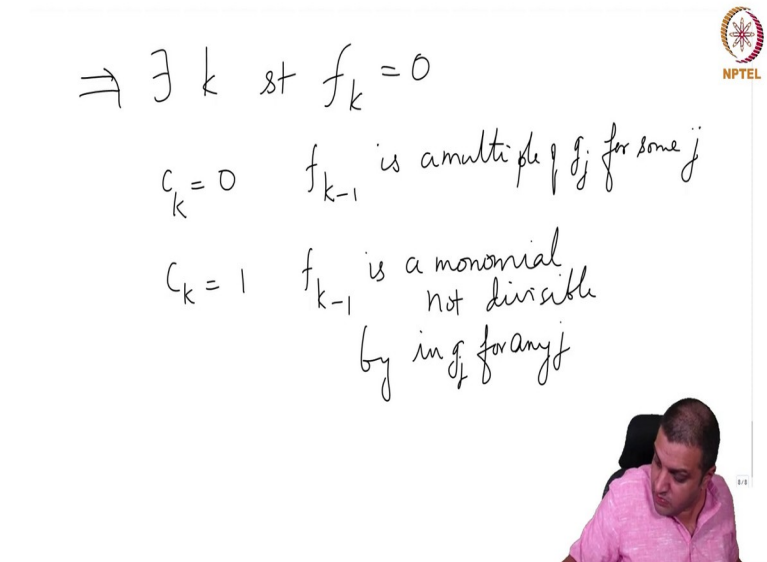
So, now repeat this, just continue constructing this. So, then we ask the same question, if there is a  $j$  such that  $\text{in}(g_j)$  divides  $\text{in}(f_1)$ , then modify get an  $f_2$  with this property or an  $f_2$  with this property, keeping track of what  $c_2$  would be. So, let me just write it

once; define  $f_1 = f_1 - \dots \frac{\text{in}(f_1)}{\text{in}(g_j)} g_j$ , if there exist  $g_j$ , such that  $\text{in}(g_j)$  divides  $\text{in}(f_1)$  otherwise we will just write  $f_2 = f_1 - \text{in}(f_1)$ . And as earlier for this one we write  $c_2 = 0$ ; here we said  $c_1 = 0$  this is the modification and with the modification is just blindly removing the leading term, then just call it  $c_2 = 1$ . So, repeat this and then we ask if  $f_2$  is non-zero and so on. So, if  $f_2 \neq 0$ ,  $\text{in}(f_2) < \text{in}(f_1)$ .

So, now we saw this proof earlier, this cannot go on forever. So, this cannot go for forever; because otherwise we would get a no infinite descending chain of monomials. This we proved in the course of proving Hilbert basis theorem, we made this

observation. So, this cannot go on forever. So, now, what was that mean? It means that at some stage  $f_k$  is 0.

(Refer Slide Time: 13:35)



$\Rightarrow \exists k \text{ st } f_k = 0$   
 $c_k = 0 \quad f_{k-1} \text{ is a multiple of } g_j \text{ for some } j$   
 $c_k = 1 \quad f_{k-1} \text{ is a monomial not divisible by } \text{in}(g_j) \text{ for any } j$

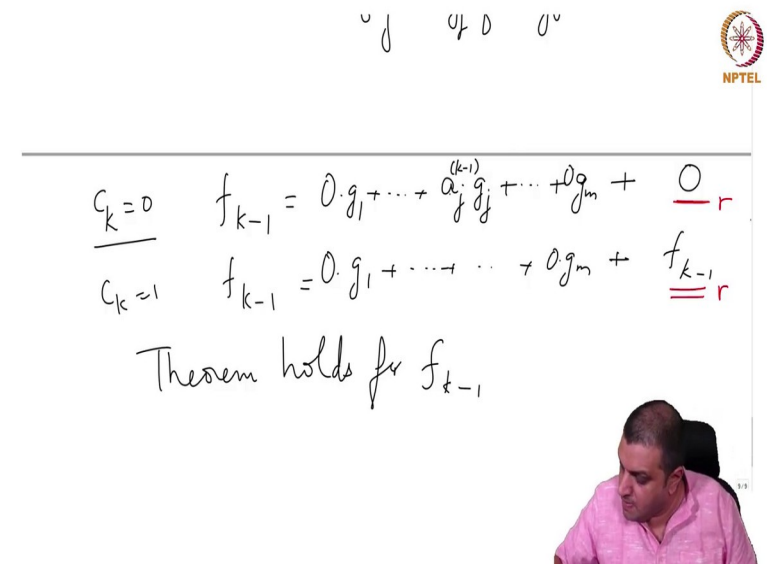
So, this now implies that, there exists a  $k$  such that  $f_k = 0$ . So, now we ask, what is  $f_{k-1}$ ? So, of course, to go from  $f_{k-1}$  to  $f_k$ , we would have had to make a choice which is like this; If it is not divisible by  $\text{in}(g_j)$  for any  $j$ , this is the change that we would have done; and this data is kept tracked in for constructing  $f_k$  this data will be kept tracked in  $c_k$ .

So, let us use that information. So, two possibilities; if  $c_k$  is 0. So, let us look at this way, is 0 means this is the change that we would have done; and in other words  $f_{k-1}$  is a multiple  $g_j$ , for some  $j$ ,  $c_k = 1$ . So, let us just go back here,,  $c_k = 1$  would mean that  $f_k$  was obtained by just removing the leading term of  $f_{k-1}$ ; in other words  $f_{k-1}$  is a monomial not divisible by  $\text{in}(g_j)$  for any  $j$ .

So, this is how we would write. So, now, the point is each time we see a term like this, we will keep it with the remainder; each time we see a term like this, we will add that to

the sum of  $a_i g_i$ . So, that is the idea. So, now, let us write this thing properly,. So, how do we write? So, this is just description.

(Refer Slide Time: 16:11)



$$\begin{aligned} \underline{c_k = 0} \quad f_{k-1} &= 0.g_1 + \dots + a_j^{(k-1)} g_j + \dots + 0.g_m + \underline{0} \text{ } \underline{r} \\ c_k = 1 \quad f_{k-1} &= 0.g_1 + \dots + \dots + 0.g_m + \underline{f_{k-1}} \text{ } \underline{r} \end{aligned}$$

Theorem holds for  $f_{k-1}$

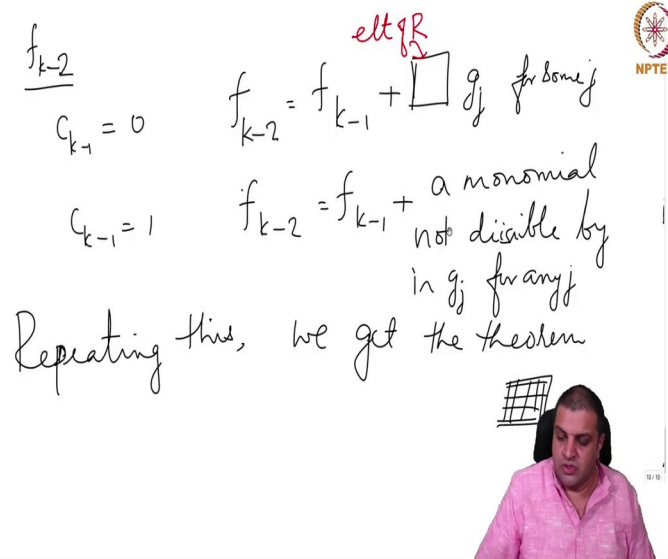
So, in this in the language of the theorem we would write; if  $c_k = 0$ . So, notice  $c_k = 0$  means, this is a multiple of that. So, we would write

$f_{k-1} = 0.g_1 + \dots + a_j^{(k-1)} g_j + \dots + 0.g_m + 0$ , 0 is the standing for the remainder, the r. If  $c_k = 1$ , then we would just write  $f_{k-1} = 0.g_1 + \dots + 0.g_m + f_{k-1}$

So, notice that this is what r is and this gives what r. So, it is gone write  $f_k$  in the fashion what the theorem wants. So, theorem holds for  $f_{k-1}$ . Let us just do one more step and then we will work out an example.



(Refer Slide Time: 18:05)



Handwritten notes on a whiteboard:

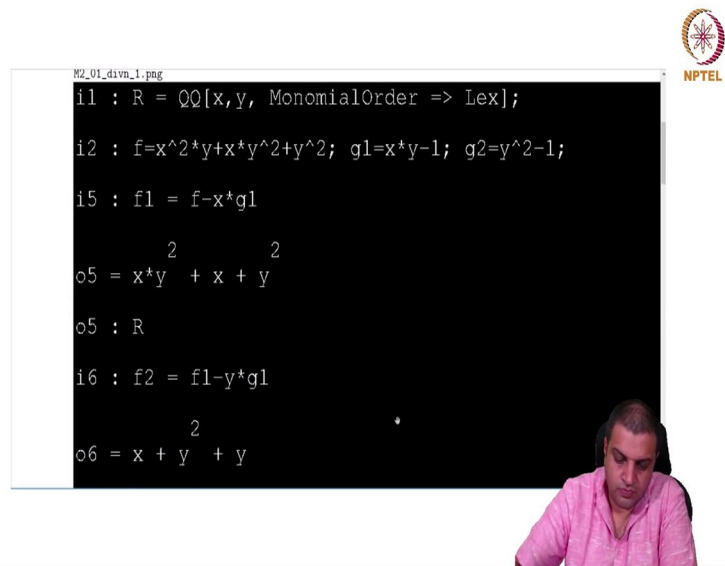
$\frac{f_{k-2}}{c_{k-1} = 0} \quad f_{k-2} = f_{k-1} + \boxed{\text{elt } g_j} g_j \text{ for some } j$   
 $c_{k-1} = 1 \quad f_{k-2} = f_{k-1} + \text{a monomial not divisible by } \text{in}(g_j) \text{ for any } j$   
 Repeating this, we get the theorem

The video feed shows a lecturer in a pink shirt.

Let us, let us ask about  $f_{k-2}$ . So, now, what we have to ask is? So, if  $c_{k-1} = 0$ ; So, we would have written  $f_{k-2} = f_{k-1} + \dots g_j$ . So, this box here says element of  $R$ . And if  $c_{k-1} = 1$ , then  $f_{k-2} = f_{k-1} + \text{a monomial not divisible by } \text{in}(g_j) \text{ for any } j$ .

So, now you can go back to this sort of a construction,  $f_k$  has its property; so now, if  $c_{k-1} = 0$ , then  $f_{k-1}$  plus a multiple. So, then a coefficient here would have not changed; if this is the  $c_{k-1} = 1$ , then then this part would have changed. So, in other words depending on the value of  $c_{k-1}$ ; either the coefficients of  $g_j$  in this half of the expression would have changed or the remainder would have changed. So, repeating this we get, we get the theorem. So, that is simple.

(Refer Slide Time: 21:35)



```


i1 : R = QQ[x,y, MonomialOrder => Lex];
i2 : f=x^2*y+x*y^2+y^2; g1=x*y-1; g2=y^2-1;
i5 : f1 = f-x*g1
      2      2
o5 = x*y  + x + y
o5 : R
i6 : f2 = f1-y*g1
      2
o6 = x + y + y

```

So, now I would just like to illustrate this proof using a Macaulay's example. So, here  $R$  is a polynomial within two variables; monomial order as Lex, and  $f = x^2y + xy^2 + y^2$ ,  $g_1 = xy - 1$ , and  $g_2 = y^2 - 1$ . Now, so we are going to solve go through that algorithm;  $f$ 's leading term is  $x^2y$ ,  $g_1$ 's leading term is  $xy$ , so we multiply by  $x$  subtract. So, this is the situation where  $c_1 = 0$ ; this is how we modify it. So, we get a new polynomial, this one is leading term is  $xy^2$  that is again divisible by this leading term, so by multiplying by  $y$ . So, we modify to get  $f_2$  to be this.

This is again this, the  $c_2 = 0$ . So, this is the modification.


(Refer Slide Time: 22:38)



```
i6 : f2 = f1-y*g1
      2
o6 = x + y  + y
o6 : R
i7 : f3 = f2-x
      2
o7 = y  + y
o7 : R
```

So, now we get  $x+y^2+y$ , its leading term is  $x$ ; this is Lex, so this is the leading term, it is not divisible by the leading terms of the any of the  $g$ 's. So, which is removed that leading term and defined; so we write  $f_3$  as  $f_2 - x$  and this is a case where the change  $c_k = 1$ . So, in the previous two stages it was 0, now which is 1. So, we just forcibly removed the initial term.

(Refer Slide Time: 23:16)



```
M2_02_divn_2.png
i8 : f4 = f3-g2
o8 = y + 1
o8 : R
i9 : f == (x+y)*g1 + g2 + (x+y+1)
o9 = true
```

So, we get  $y^2$  whose leading term is divisible by this leading term. So, then we subtract the  $f_3$  and  $g_2$  to the same leading term, same coefficients also; so we subtract it and we get  $y+1$ . So, this is an expression in which no term is divisible by any of the leading terms. And if you do two more steps, we would get zero and now we can work backwards. What  $f_4$  is of the form no term is divisible by any of the initial terms, so that is put in the remainder part. Now let us go back.

Here the change is 1; in other words we got forcibly removed a leading term, so put that in the reminder. So, we got x, this  $y+1$  and the x from the previous step. So, now, now we are in this stage where there is a multiplication by sorry, one more stage; yeah there is a multiplication by y,  $y g_1$  and  $x g_1$ . Going from this to the previous stage is subtracting a multiple of  $g_2$ , that is because any. So, that would be added in this part.

So, minus  $g_2$  would here would be plus  $g_2$  and then  $y+1$  was this; the previous step we got forcibly removed an initial term x, so that goes to the remainder term and then we do two more steps, we get an  $y g_1$  and an  $x g_1$ . So  $y g_1$  from here and an  $x g_1$  from there and that is the. So, that is how the algorithm work, and this is exactly how the proof would be almost. So, this is the end of this lecture and in the next lecture we will introduce this notion called Gröbner basis and use them see some basic examples of those.