

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

**Lecture – 08**  
**Grobner basis**

Welcome to the 8th lecture in this course. So, in this lecture we are going to look at Grobner basis and use it to do some elementary, but basic computations.

(Refer Slide Time: 00:28)

Defn. Let  $I$  be an  
R ideal.  
A subset  $G \subseteq I$  is  
called a **Grobner basis**  
of  $I$  (w.r.t  $>$ ) if  
 $|G| < \infty$  and

$R = k[x_1, \dots, x_n]$   
 $k$  field.  
 $>$  monomial  
order on  $R$



So, throughout we call that  $R$  is a polynomial ring in  $n$  variables over a field  $k$  and Let  $I$  be an  $R$  ideal oh sorry one more point, this is a monomial order on  $R$ ; there is an underlying monomial order which and we will always refer to initial ideal etcetera with respect to that. So, a subset  $G$  inside  $I$  is called a Grobner basis of  $I$ . Again this is with respect to the given order if.

(Refer Slide Time: 02:05)



$$\text{in}_> I = \{ \text{in}_> g \mid g \in G \}$$

Remark: Every ideal has a Grobner basis.



So, if  $G$  is finite and the initial ideal of  $I$  is generated by the set  $\text{in}_>(g)$ , where  $g$  is from this finite set. So, it is a finite subset of the ideal whose initial terms generate the initial ideal of  $I$ . So, that is the thing is called a Grobner basis. So, remark that every ideal has as such every ideal has a Grobner basis.

That is because initial ideal is finitely generated. Generated by some  $\text{in}_>(g_1), \text{in}_>(g_2)$  or up to some  $m$  elements, then by Grobner basis we mean the set  $g_1$  through  $g_m$ . So, every ideal has a Grobner basis. And what we wanted to prove is that a Grobner basis of an ideal is a generating set for the ideal.

So, after we prove that statement how we can think about Grobner basis is, it is a generating set whose initial terms generate the initial ideal also. So, it is not just a generating set. So, before we do that, we need to prove small lemma which is reminiscent of the uniqueness of the remainder when we divide in the one variable case.

(Refer Slide Time: 03:53)



Lemma: Let  $I$  be an ideal  
&  $G = \{g_1, \dots, g_m\}$  a Grobner basis for  $I$ .  
Let  $f \in R$ . Suppose that  
$$f = \sum a_i g_i + r$$
$$f = \sum a'_i g_i + r'$$



So here is the Lemma, let  $I$  be an ideal and  $G$  some  $\{g_1, \dots, g_m\}$  a Grobner basis for  $I$ . Let  $f$  be inside  $R$ . Now we know from the division algorithm from the previous lecture that we can write  $f$  as  $\sum a_i g_i + r$ . But we could possibly have written it in a different way also the same  $g_i$  plus; but the coefficients might be different and also the remainder this the term  $r$  might be different.

(Refer Slide Time: 05:08)



are two expressions that satisfy  
the conclusion of the theorem  
about the division algorithm.

Then  $r = r'$

Proof: 
$$0 = \sum_{i=1}^m (a_i - a'_i) g_i + (r - r')$$



So, suppose that these two this and this are two expressions such that that satisfy the conclusion of the division algorithm, conclusion of the theorem about the division algorithm. So, what does that let me just say instead of writing it. So, here it means that  $r$  is 0 or no term of  $r$  is divisible by  $\text{in}(g_i)$  for any  $i$ .

Similarly,  $r'$  is 0 or no term of  $r'$  is divisible by  $\text{in}(g_i)$  for any  $i$ . So, this is what the conclusion of the theorem was that there is such an  $r$ , then  $r$  equals  $r'$ . There is no guarantee about the coefficients of the  $g_i$  the  $a_i$  need not be equal to  $a'_i$ , but the remainder is uniquely determined. But what we have to use in the prove that this is it is a Grobner basis. So, we will see how it is done.

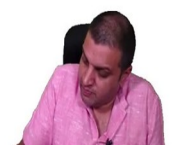
So, let us so proof this is not very difficult at all. So, note that we just subtract one from

the other and we would get  $0 = \sum_{i=1}^m (a_i - a'_i) g_i + (r - r')$  now. So, this  $g_i$ 's are from the Grobner basis of  $I$ . So, this expression on the left the first expression here is in the ideal, hence this is also in the ideal.

(Refer Slide Time: 07:43)



Therefore  $r - r' \in I$ .  
 If  $r - r' \neq 0$ ,  
 then  $\exists j$  st  $\text{in}_j g_j \mid \text{in}_j (r - r')$   
 Obv:  $\text{in}_j (r - r')$  is a term  
 of  $r$  or of  $r'$



Therefore  $r - r'$  is in the ideal. What we want to show is that  $r - r'$  is 0. If  $r - r'$  is not 0, then there exist a  $j$  such that the initial term of  $g_j$  divides the initial term of

$r - r'$ . Now what is  $r - r'$ ? And what is the initial term of  $r - r'$ ? well we consider we write  $r$  as some polynomial with monomials and coefficients and we are subtracting the same similar expression for  $r'$ .

The initial term must have appeared either  $\text{in}(r)$  or  $\text{in}(r')$ , if you just take a difference of two polynomials some monomial that did not occur  $\text{in}(r)$  or  $\text{in}(r')$  would not suddenly show up in the difference. So, the observation is that the initial term of  $r - r'$  is a term of  $r$  or of  $r'$ . Not necessarily the initial term, because it is possible that  $r$  and  $r'$  had the same initial term and the difference canceled it. So but however whatever the nonzero; if this is nonzero it is initial term must have occurred either  $\text{in}(r)$  or  $\text{in}(r')$ .

(Refer Slide Time: 09:29)

Hence  $\text{in}(g_i)$  divides a term  
of  $r$  or of  $r'$ , contradiction  
Hence  $r = r'$



And hence  $\text{in}(g_i)$  divides some term of  $r$  or  $r'$ , hence  $\text{in}(g_i)$  divides a term of  $r$  or of  $r'$ , which is a contradiction and the contradiction was with the assumption that if this is nonzero. Hence  $r$  equals to  $r'$ . So, we did use then it is a Grobner basis here.

So, it is not true for arbitrary generating sets for  $I$ , it is only true when we work with Grobner basis. So, just one this is the end of them this lemma.

(Refer Slide Time: 10:30)



Defn. Let  $I$  be an ideal &  $G$  a Grobner basis of  $I$ . Let  $f \in R$ .  
The elt  $r \in R$  obtained from the division algorithm (same notation as in that theorem) is called the remainder of  $f$



So just may be one definition, let  $I$  be an ideal and  $G$  a Grobner basis of  $I$ . Let  $f$  be in  $R$ . So now, we know that if you apply the division algorithm to  $f$  and divided by the elements of  $G$ . The element  $r$  in  $R$  obtained from the division algorithm, I mean same notation is about as in that theorem is called the reminder remainder of  $f$  and it is denoted by

(Refer Slide Time: 12:20)



And is denoted by  
 $rem_G(f)$



$rem_G(f)$  when we divide by the set  $G$  and this again this make sense only when  $G$  is a Grobner basis of an ideal. So, before we apply this this theorem this result for a for a first

application of study in Grobner basis, I just want to make just one remark let us go back here.

(Refer Slide Time: 12:56)

Remark. We ~~do~~<sup>NOT</sup> need to know  $I$  in the above statements

Required:  $G \subseteq R$  st  
 $G$  is a Grobner basis  
for the ideal it generates



So, in this definition or in the previous proposition we took an ideal and then took a Grobner basis. But however, nowhere in the statement do we refer to the ideal itself, it is always some statement about  $G$  and  $f$  and so on. So, if you so we really do not have to take an ideal to start with, all that we have to say is if  $G$  is a we do not need to know  $I$  in the above statements.

What is required is a following property is that  $G$  is a subset of  $R$ , such that  $G$  is a Grobner basis for the ideal it generates;  $G$  is the subset of  $R$ . It is of course, going to generate some ideal. It is all that we need is the  $G$  is a Grobner basis for the ideal it generates and we do not need to know what that ideal is and as we learn more about Grobner basis or given some set of polynomials how do you find a Grobner basis that it generates when we study that algorithm later. We will see that this is a statement that can be checked without knowing what the ideal is.

So just keep this in mind, although I stated those things for ideal that is because till then we had not really thought about the property of a subset as being a Grobner basis it was always with respect to an ideal. But it is in  $I$  mean we do not need to explicitly refer to the ideal all the time.

(Refer Slide Time: 15:00)

Ideal membership test.



So anyway, so here is what is called the Ideal membership test. Maybe before I do that let me sorry I we did this in the last lecture.

(Refer Slide Time: 15:49)

From the last lecture:  
$$\frac{\text{If } G \subseteq I \text{ st } \{in(g) | g \in G\} \text{ generates in } I, \text{ then } G \text{ generates } I}{G \text{ is a Grobner basis of } I}$$



But let me just remind you from the last lecture this is the proof of Hilbert basis theorem.

What we really proved is that if  $G$  is a subset in  $I$  such that  $\{in(g) : g \in G\}$  generates in  $I$ , then  $G$  generates  $I$ . This is this was our concrete proof of Hilbert basis theorem that  $I$  as a finite generating set. So, what is this? This is just saying  $G$  is a Grobner basis right. So



this statement in the language that we have introduced today. So, just as  $G$  is a Grobner basis of  $I$ .

So, any Grobner basis of  $I$  is already a generating set for  $I$ . But it has a following useful property called ideal membership test.

(Refer Slide Time: 17:03)

Propn. (Ideal membership test) Let  $I$  be an ideal &  $G \subseteq I$  a Grobner basis for  $I$ .  
Let  $f \in R$ . Then  
$$f \in I \iff \text{rem}_G(f) = 0$$



Let us learn that now proposition ideal membership test. Let  $I$  be an ideal and  $G$  inside  $I$  a Grobner basis for  $I$ . Then let  $f$  be an element of  $R$ .

We want to test whether  $f$  is inside  $I$  or not, then  $f$  is inside  $I$  if and only if  $\text{rem}_G(f)$  is 0. So, this again it works for first of all to make sense of remainder of when divided by  $G$ ,  $G$  must be a Grobner basis the assumed the remainder part of the  $r$  in the division algorithm at the end is unique, when we work with a Grobner basis. So, this is this is well defined and then we can ask this question. So, this is what is called the ideal membership test and this is one of the first applications immediate applications of the theory of Grobner basis proof.

(Refer Slide Time: 18:50)



Proof  $(\Leftarrow):$   $\text{rem}_G(f) = 0$

$$\Rightarrow \exists a_i \text{ s.t. } f = \sum a_i g_i + 0$$

$$\therefore f \in I$$



So, let us prove the if part. the reminder of  $f$  is 0, implies that there exists  $a_i$  such that  $f$  is  $\sum a_i g_i + 0$  this is this thing. so it is 0. So, in other words therefore  $f$  is inside  $I$ , the  $g_i$ 's are inside  $I$ , any linear combinations inside  $I$ , so  $f$  is inside  $I$ .

So, this is the easy part one did not really use that it is a Grobner basis except to say that yeah this part.

(Refer Slide Time: 19:50)



$(\Rightarrow)$ . Let  $f \in I$ .  $r = \text{rem}_G(f)$

BWOC, assume that  $r \neq 0$ .

$$r = f - \sum a_i g_i \in I$$

$$\Rightarrow \text{in}_>(r) \in I, \Rightarrow \exists g \in G$$

$$\text{in}_>g \mid \text{in}_>(r). \quad \left( \begin{array}{l} \because G \text{ is a} \\ \text{Grobner basis} \end{array} \right)$$



So, let us move the other direction. So, let  $f$  be inside  $I$ . So, by way of contradiction assume that remainder, so let us maybe; let us write  $r = \text{rem}_G(f)$  let us assume that  $r$  is nonzero.

So, but what is  $r$ ?  $r$  is  $f - \sum a_i g_i$  this is also inside  $I$  mean this is inside  $I$  irrespective of whether 0 or not, 0 is also inside  $I$  this is there. In other words the initial term, so now is where it is non zero is used,  $\text{in}(r)$  is inside  $I$ . Which means that there exist (Refer Time: 21:19) a  $g$  inside  $G$  such that  $\text{in}(g)$  divides  $\text{in}(r)$ . That is because it is a Grobner basis; since  $G$  is a Grobner basis.

(Refer Slide Time: 21:53)

This contradicts the  
conclusion of the  
division algorithm.

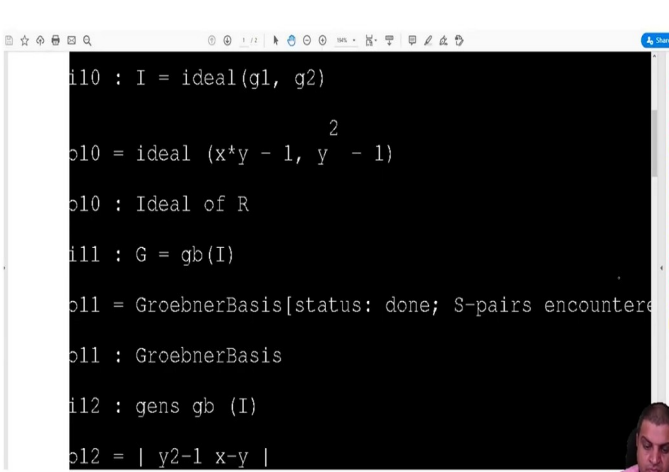
$$\Rightarrow r = 0$$



So, this contradicts the conclusion of the division algorithm, I mean sorry whenever I say division algorithm I mean the theorem in which we prove the algorithm, we did not explicitly write down the algorithm ourselves conclusion of the division algorithm. So and why did we get this conclusion at the contradiction the contradiction was the from this assumption that  $r$  is non zero.

In other words, this is what we wanted to prove. So, ideal membership test is the one of the one of the first applications one learns after one becomes familiar with Grobner basis. So, let us just look at the stuff that we discussed in this lecture let us look at in Macaulay. So, here is the how the Grobner Basis is calculated.

(Refer Slide Time: 22:53)



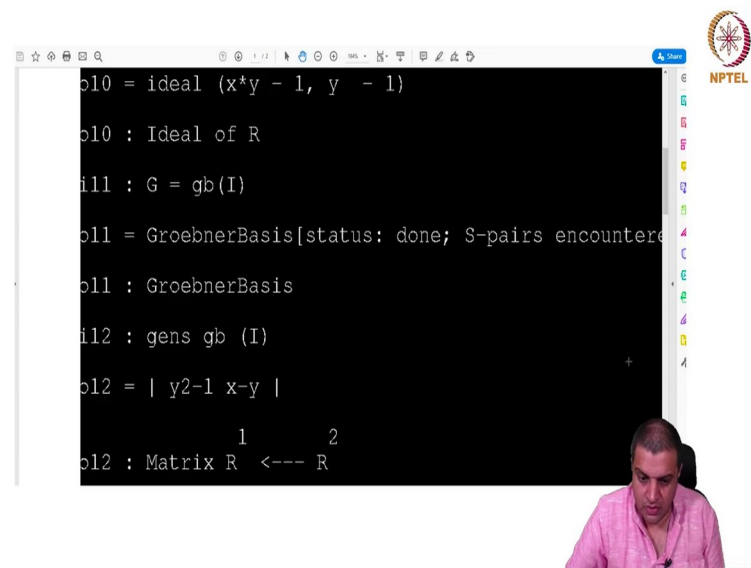
```
i10 : I = ideal(g1, g2)
p10 = ideal (x*y - 1, y^2 - 1)
p10 : Ideal of R
i11 : G = gb(I)
p11 = GroebnerBasis[status: done; S-pairs encountered]
p11 : GroebnerBasis
i12 : gens gb (I)
p12 = | y^2-1 x-y |
```

So, again this is back in same example that we were discussing in the last lecture  $R = k[x, y]$  Lex order and  $g_1 = xy - 1$ ,  $g_2 = y^2 - 1$  and we just call I the ideal of; then we asked Macaulay to compute the GrobnerBasis.

So the command is gb, so  $G = gb(I)$ . So, it does not just give you the list of the elements in the GrobnerBasis, it keeps track of some other extra structure. So, it outputs what is called an object of GrobnerBasis class and there is some diagnostic message how. So, we will discuss what S- pairs are etcetera are later.

So, anyway there is some diagnostic messages that we can ignore for now. It returns at returns to us an object of Grobner basis class. If you want to actually know what is the GrobnerBasis, then we can ask  $gens gb(I)$ .

(Refer Slide Time: 24:05)



```
p10 = ideal (x*y - 1, y^2 - 1)
p10 : Ideal of R

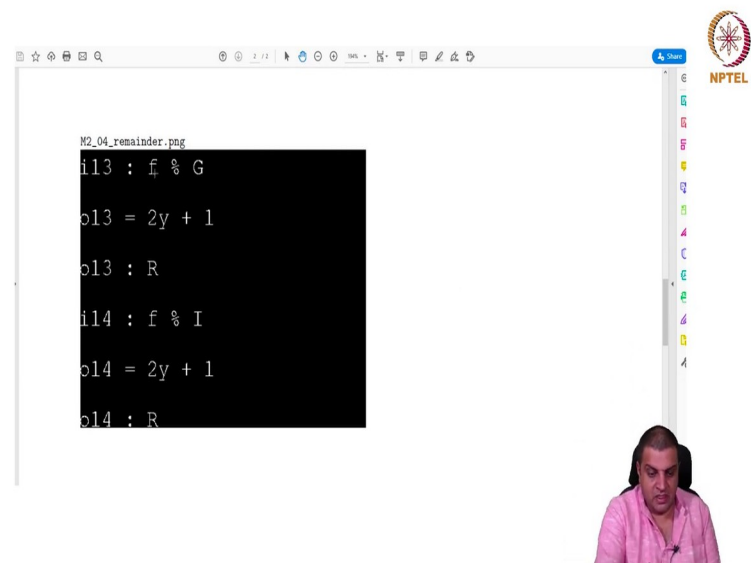
i11 : G = gb(I)
p11 = GroebnerBasis[status: done; 3-pairs encountered]
p11 : GroebnerBasis

i12 : gens gb (I)
p12 = | y^2-1 x-y |
      1      2
p12 : Matrix R <--- R
```

So, it says  $y^2-1$  and  $x-y$ . So, that  $x-y$  is there in this ideal was not obvious by looking at this, I mean we can calculate  $-x(y^2-1)+y(xy-1)=x-y$ .

So, this is there and it says this is a GrobnerBasis. So now let us look at some ideal membership tests yeah.

(Refer Slide Time: 24:45)



```
N2_04_remainder.png
i13 : f % G
p13 = 2y + 1
p13 : R

i14 : f % I
p14 = 2y + 1
p14 : R
```

So, the same f from last lecture and the symbol is percentage sign to reduce modulo GrobnerBasis.

So, we can do it in two different ways we can ask  $f$  reduce modulo  $G$ ; then we will say this is the remainder or we could just give an ideal and then we will get this remainder. And in the exercises we will try to understand these things a little bit more. So, this is the end of this lecture. And in the next one we will start looking at further applications in solving polynomial equations.