
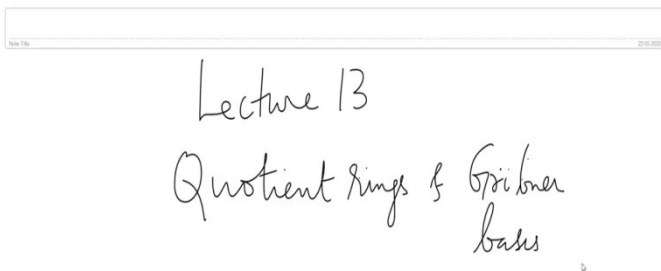



**Computational Commutative Algebra**  
**Prof. Manoj Kummini**  
**Department of Mathematics**  
**Chennai Mathematical Institute**

**Lecture - 13**  
**Monomial basis**

(Refer Slide Time: 00:16)



Welcome, this is lecture 13 in the series. We will look at the Application of Grobner basis to describe Quotient Rings, and then use it as a way to look at to determine whether system of polynomial equations have finitely many solutions, the solution that is finite. So, here is a proposition which is sort of the one of the important reasons for studying, I mean among the one of the original motivations for studying this.



Then  $\{m \text{ monomial in } R \mid m \notin \text{in}(I)\}$   
is a  $k$ -vector space basis of  $R/\underline{I}$ .



Note:  $R$  is a  $k$ -vector space.  
A basis for  $R$  is the set of monomials.  
 $I$  is  $k$ -vector subspace of  $R$ .  
 $R/I$  is a  $k$ -vector space.

Just let us make sure we understand what this means. Note,  $R$  is a  $k$ -vector space. A basis for  $R$  is the set of monomials.  $I$  is a  $k$ -vector subspace of  $R$ . Therefore,  $\frac{R}{I}$  is a  $k$ -quotient vector space.

Now, monomials need not form a basis for  $I$ , because  $I$  could be generated by non-monomial polynomials. So, this may not have a basis of monomials. However, the quotient ring has a basis of monomials which comes precisely from the complement of  $I$ . So, that is the proposition. So, we will prove this.

(Refer Slide Time: 03:47)

Proof: Let  $G$  be a Grobner basis for  $I$ .

linear independence

$$\sum_{\text{finite}} \alpha_i m_i = 0 \quad \left. \begin{array}{l} m_i \notin \langle I \rangle \\ \alpha_i \in k \end{array} \right\}$$

$\Leftrightarrow \sum \alpha_i m_i \in I$

$\Rightarrow \text{in}_>(\sum \alpha_i m_i) \text{ is divisible by } \text{in}_>g \text{ for some } g \in G$



So, you have to prove that a subset is a basis for a vector space. So, we have to prove two things, we have to prove that it spans and it is linearly independent. So, let  $G$  be a Grobner basis for  $I$ .

Now, let us prove the first case: linear independence. Suppose, we have some  $\sum_{\text{finite}} \alpha_i m_i = 0$ ,  $m_i \notin \langle I \rangle$  for all  $i$ , and  $\alpha_i \in k$ . So, a  $k$  linear combination of elements in this potential set, say

let us say it is 0. So, this is 0 in  $\frac{R}{I}$ .

So just when we write  $\sum \alpha_i m_i = 0 \in \frac{R}{I}$  we mean the residue class inside  $\frac{R}{I}$ , but here I mean the actual monomial itself the same sum is inside  $I$ ; which means that the initial term of the sum is divisible by  $in_i g$ , for some  $g \in G$ .

Now, what is the initial term of this? These are monomials, these are distinct monomials, there are no cancellation among them, the one that is the largest.

(Refer Slide Time: 06:23)

$\Rightarrow$  If  $\alpha_i \neq 0$  for some  $i$ ,  
then  $\exists m_j \notin in(I)$  divisible by  
 $in(g)$  for some  $g \in G$   $\rightarrow$  ~~x~~  
 $\therefore \alpha_i = 0 \forall i$



If  $\alpha_i \neq 0$  for some  $i$ , then there exists  $m_j \notin in_i I$  divisible by  $in_i g$ , for some  $g \in G$ . But this is not possible.

Anything that is divisible by  $g$  by such terms will be inside here. So, this is a contradiction. This contradiction is for this assumption. So, therefore,  $\alpha_i = 0$  for all  $i$ , which is what we wanted to prove. This proof for linear independence.

(Refer Slide Time: 07:53)



Spanning: Let  $f \in R$ .  
Let  $r = \text{rem}_G(f)$   
 $f - r \in I$ .  
 $f \bmod I = r \bmod I$ .  
No term of  $r$  is divisible by  $\text{img}$   
for any  $g \in G$ .



Now, we would like to prove that the set spans the vector space. So, let  $f \in R$ , and apply the division algorithm. Let  $r$  be equal to the remainder of  $f$  under division by  $G$ . Notice that  $f - r$  is a sum of linear combinations of the  $G$ , so it is inside  $I$ .

So, in other words,  $f \bmod I = r \bmod I$ . But what is the property of  $r$ ?  $r$  has a property that no term of  $r$  is divisible by  $\text{img}$ , for any  $g \in G$ .

(Refer Slide Time: 09:17)



No term of  $r$  is divisible by  $\text{img}$   
for any  $g \in G$ .

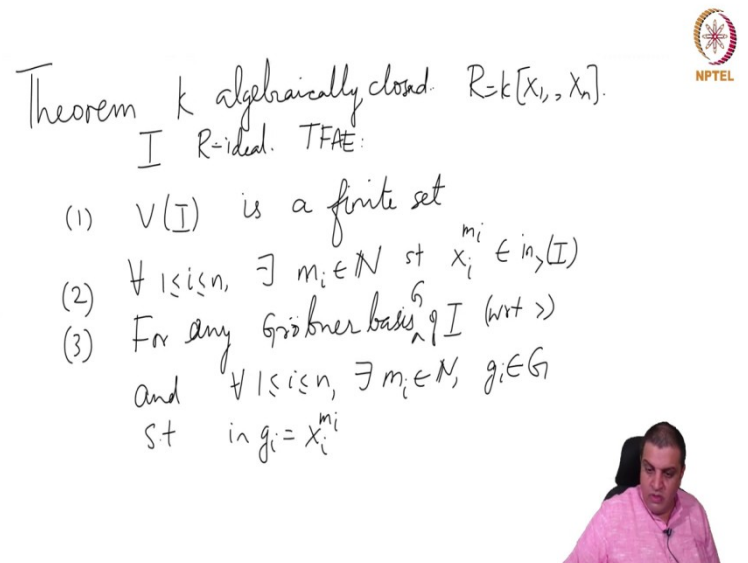
i.e.,  $r \in \text{Span} \{ \text{monomial in } R \mid m \notin I \}$



So, in other words  $r$  is in the span of that set monomials, so we can write it  $r \in \text{Span}\{m \mid m \text{ monomial} \in R \mid m \notin I\}$ . Therefore, it spans and hence the proof is done. So, this is the property of this description of quotient rings and its relation to Grobner basis of  $I$ .

So, with this we can use this idea, result to prove the following theorem.

(Refer Slide Time: 10:05)



Theorem  $k$  algebraically closed  $R = k[X_1, \dots, X_n]$ .  
 $I$   $R$ -ideal. TFAE:

- (1)  $V(I)$  is a finite set
- (2)  $\forall 1 \leq i \leq n, \exists m_i \in \mathbb{N}$  st  $X_i^{m_i} \in I$
- (3) For any Grobner basis  $G$  of  $I$  (wrt  $>$ )  
 and  $\forall 1 \leq i \leq n, \exists m_i \in \mathbb{N}, g_i \in G$   
 st  $\text{in } g_i = X_i^{m_i}$

This is about finiteness of the solution set throughout. So, now we assume  $k$  algebraically closed. We may not need to assume  $k$  algebraically closed, but since we did not describe how to translate or what is the relation between arbitrary field and its algebraic closure when we work in these things, it is better to assume algebraically closed and have a clean statement now.  $R = k[X_1, X_2, \dots, X_n]$ ,  $I$  is an  $R$ -ideal, then the following are equivalent.

One,  $V(I)$  which is the common zeroes of all the polynomials in  $I$  is a finite set. Two,  $\forall 1 \leq i \leq n, \exists m_i \in \mathbb{N}$  such that  $X_i^{m_i} \in I$ . So, fix any monomial order, the result does not depend on the monomial order itself. Three, for any Grobner basis  $G$  of  $I$ , again with respect to the given monomial order and for all the same quantifier for each variable it means,  $\forall 1 \leq i \leq n, \exists m_i \in \mathbb{N}, g_i \in G$  such that  $\text{in}(g_i) = X_i^{m_i}$ .

(Refer Slide Time: 13:00)



(4)  $\{m \text{ monomial in } R \mid m \notin I\}$  is finite

(5)  $\dim_k(R/I) < \infty$

Proof: (2)  $\Leftrightarrow$  (3) ✓

(4)  $\Leftrightarrow$  (5) previous proposition

Need to show: (1)  $\Rightarrow$  (2), (3)  $\Rightarrow$  (4), (5)  $\Rightarrow$  (1)



Statement four, the set  $\{m \text{ monomial in } R \mid m \notin I\}$  is finite. And five, the dimension as a  $k$ -vector space of  $\frac{R}{I}$  is finite.

So, let us look at these statements just once more. So, we are trying to understand when would the zero set of  $I$  be finite that is a first statement. Second statement says something about some nice terms powers of variables inside the initial ideal. Third is just restatement of two that in any Grobner basis there is a polynomial in which a power of a variable is the initial term. And four is the complement of the initial ideal in the set of monomials and their complement is finite. And five, dimension of this is as a  $k$ -vector space is finite.

So, in the proof let us finish off the ones that are that we already know. Let us look at 2 and 3. 2 says there is an  $X_i^{m_i}$  in the initial ideal which means that in every Grobner basis there is an element in the basis whose leading term is  $X_i^{m_i}$ . So, that says 2 implies 3, and if 3 is true, clearly 2 is true because this initial term shows up there. So, 2, if and only if 3 is from the definition of a global basis; so, this we will not reprove.

What about 4 and 5? So, that is the previous proposition. This set is a  $k$ -vector space basis for this. So, this is finite if and only if this is finite dimensional.

So, for if and only if 5 is the previous proposition. So, what we will prove now is 1 implies 2, 3 implies 4, and 5 implies 1. So, what we will show and that is enough 1 implies 2, 3 implies 4, and 5 implies 1. If you prove these statements everything will be done.

(Refer Slide Time: 16:35)



(1)  $\Rightarrow$  (2).  $V(I)$  is a finite set.

Fix  $1 \leq i \leq n$

Let  $A_i \subset k$  be the values of the  $i$ -th coordinate of the pts in  $V(I)$

$$|A_i| < \infty$$

$$f_i(X_i) := \prod_{a \in A_i} (X_i - a)$$



So, let us prove 1 implies 2. So,  $V(I)$  is a finite set. So, fix an  $i$  such that  $1 \leq i \leq n$  and let  $A_i \subset k$  be the values of the  $i$ -th coordinate of the points in  $V(I)$ . So, just project  $V(I)$  to the  $i$ -th coordinate and just pick out those the image of that thing. So,  $A_i$  is a finite set. Define the polynomial  $f_i(X_i) := \prod_{a \in A_i} (X_i - a)$ .

(Refer Slide Time: 18:03)



Note that  $f_i \in I(V(I)) = \sqrt{I}$

$$\Rightarrow (f_i)^{k_i} \in I \text{ for some } k_i$$

$$\text{in } (f_i)^{k_i} = X_i^{|A_i|k_i} \in \text{in}_i(I)$$

(3)  $\Rightarrow$  (4) Notice that  $X_1^{a_1} \dots X_n^{a_n} \notin \text{in}_s(I)$

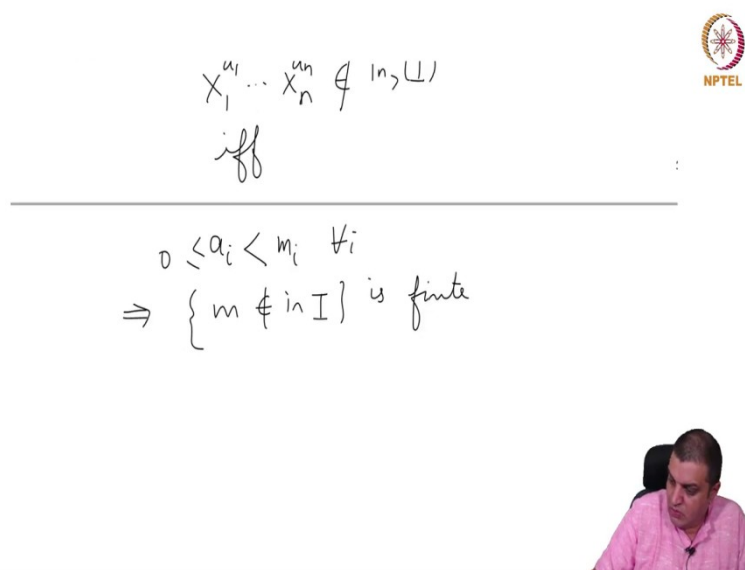




Notice that  $f_i$  vanishes at everywhere inside  $I$ . Note that the  $i$ -th coordinate of any point in  $V(I)$  will be from  $A_i$ . So, it would vanish, so that  $f_i \in I(V(I)) = \sqrt{I}$ . This is the radical of  $I$  that we proved.

So, what does that now mean? It means now that  $f_i^{k_i} \in I$  for sum  $k_i$ . But what is  $f_i^{k_i}$  look like? So, the initial term of  $f_i^{k_i}$  is that is quickly. So, the degree of  $f_i$  is the cardinality of  $A_i$  and  $\text{in}_{\mathfrak{c}}(f_i^{k_i}) = X_i^{i A_i \vee k_i} \in \text{in}_{\mathfrak{c}}(I)$  and this is true for every  $I$ . So, this proves that 1 implies 2.

(Refer Slide Time: 19:51)



$$X_1^{a_1} \dots X_n^{a_n} \notin \text{in}_{\mathfrak{c}}(I)$$

iff

---


$$0 \leq a_i < m_i \quad \forall i$$

$$\Rightarrow \{m \notin \text{in } I\} \text{ is finite}$$

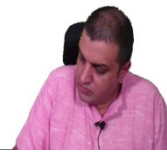
We already observed 2 implies 3. Now, let us prove 3 implies 4. So, an arbitrary monomial  $X_1^{a_1} X_2^{a_2} \dots X_n^{a_n} \notin \text{in}_{\mathfrak{c}}(I)$ , that is for each  $i$ ,  $X_i^{m_i}$  divides it in the initial ideal is not in the initial ideal if and only if the  $i$ -th exponent is divisible by  $m_i$  then it is in the initial ideal because  $X_i^{m_i}$  is in the initial ideal.

So, this is true, if and only if  $0 \leq a_i < m_i$  for all  $i$  which now implies that the set  $\{m \notin \text{in}(I)\}$  is finite. There are only finitely many exponents satisfying this condition.

(Refer Slide Time: 20:34)



$$\begin{aligned} & 0 \leq a_i < m_i \quad \forall i \\ \Rightarrow & \{m \notin I\} \text{ is finite} \\ (5) \Rightarrow (1). & \text{ Fix } i. \\ \hline & \{1, x_i, x_i^2, \dots\} \text{ give} \\ & \text{a linearly dependent set in } R/I \\ \Rightarrow & \exists f_i(x_i) \in k[x_i] \text{ st } f_i(x_i) \in I. \end{aligned}$$



So, now we come to the last part which is 5 implies 1. So fix some  $i$ , let us look at  $\{1, X_i, X_i^2, \dots\}$ . So, consider the subset of monomials inside  $R$ . This give a linearly dependent

set in  $\frac{R}{I}$ , because  $\frac{R}{I}$  is finite dimensional this is countable. So, if you take the images inside

$R$  these are linearly independent, but if you take their images inside  $\frac{R}{I}$  then because  $\frac{R}{I}$  is finite dimensional there must be a linear relation among them.

So, in other words there exists some  $f_i(X_i) \in k[X_i]$  in one variable, such that  $f_i(X_i) \in I$ . This is true for every  $i$ .

(Refer Slide Time: 21:58)



$$\begin{aligned} & \text{True for every } i \\ & I \supseteq (f_1(x_1), f_2(x_2), \dots, f_n(x_n)) \\ & \text{If } \underline{a} \in V(I) \quad \underline{a} = (a_1, a_2) \\ & \quad \text{then } f_i(a_i) = 0 \\ & \Rightarrow V(I) \text{ is finite.} \end{aligned}$$



So, therefore,  $I \supseteq (f_1(X_1), f_2(X_2), \dots, f_n(X_n))$ . Now, if some point in  $k^n$  has to satisfy all of these things, the first coordinate can only take finitely many values depending on this condition, for the second coordinate and so on.

So, if  $\underline{a} \in V(I)$ , let us say  $\underline{a} = (a_1, a_2, \dots, a_n)$ , then  $f_i(a_i) = 0$  which means that  $a_i$  has to come out from a finite collection and therefore  $V(I)$  is a finite set. The point is that  $V$  of this ideal is a finite set, therefore, any ideal containing it also will be a finite set.

So, this is the this is an useful application of the things that we discussed so far for this problem about determining if there are finitely many solutions.

(Refer Slide Time: 23:22)



```

May 22, 2020

In [1]: %%macaulay2
        R = ZZ/11[x,y,z, MonomialOrder => GLex];
        I = ideal "x5+y3+z2-1, x2+y3+z-1, x4+y5+z6-1";

Ideal of R

Let us compute a Groebner basis and look at the elements.

In [2]: %%macaulay2
        G = gens gb I

| y3+x2+z-1 x5-x2+z2-z z6+x4-x2y2-y2z+y2-1 |

1      3
Matrix R <--- R

Quickly check that in(I) contains powers of the variables:

```



So, now let us look at these things in macaulay. So, again ignore this first line with some two percentage in macaulay, it just says that we are running some macaulay code. So, we are defining a polynomial ring. So, once at least in the earlier example we saw that if you switch from G Lex to Lex the complexity of computing of Grobner basis goes up substantially. So, I have used small field to to illustrate this calculation.

So, here is polynomial ring with G Lex order. Actually, it is the same polynomials that we chose earlier. We compute the Grobner basis.

(Refer Slide Time: 24:16)



```

In [3]: %%macaulay2
        leadTerm I

| y3 x5 z6 |

1      3
Matrix R <--- R

Hence  $V(I)$  is finite.
Therefore  $I$  contains polynomials  $f(x), g(y), h(z)$ 
Solve these first, and then check which of them are solutions to  $p(x, y, z) \in G$ .
In general, it is tedious to find these single-variable polynomials in  $I$ .
Here is another approach, using "elimination of variables" which will be discussed in the next
lecture in detail
Instead of GLex we use Lex.

In [4]: %%macaulay2
        R = ZZ/11[x,y,z, MonomialOrder => Lex];
        I = ideal "x5+y3+z2-1, x2+y3+z-1, x4+y5+z6-1";

```



So, this is again, the offset line is the code that is run and the line that comes from the left it says the full width line is the output. So, it computes the (Refer Time: 24:30) for the generators of the Grobner basis. So, it gave this and this one.

And we can quickly check that initializer contains powers of the variables. I mean we can do that just by directly looking at here itself initial term is  $y^3$ , initial term is  $x^2$ , initial term is  $z^6$ . So, all variables have their powers on the initial ideal which we see just by looking at here itself. So, this tells us that this  $V(I)$  is finite in this case.

Of course, we will not probably ask for it over  $\frac{\mathbb{Z}}{11}$ , but we can only discuss it over its algebraic closure, but that is ok. Computation is done in over  $\frac{\mathbb{Z}}{11}$  itself. So, therefore,  $I$  contains polynomials  $f(x)$ , polynomial that involves just  $x$ ;  $g(y)$ , this is a polynomial that involves just  $y$  and  $h(z)$  this is a polynomial that involves only  $z$ .

So, in principle to find the solutions we could just solve these one variable equations and then. So, we get some finite set and in that finite set we can explicitly check whether which of these satisfy these polynomials. Remember, these are mixed there is a  $y, x$  term there is all variables here, there is a mixture  $x^2, y^2$  term.

So, these do not fit this description. But if we can find these 3 polynomials then we can just find the superset from which the solutions will come, superset itself will be finite and then one can then just check against each one of these things which of them are actually solutions and which of them are not. So, this is theoretically possible. But it is somewhat tedious because it is not easy to identify such single variable polynomials. And we will see this in the next lecture which has to do with something about elimination.

So, we will do this. So, elimination will be discussed in the next lecture. But the unfortunate part is we have to use Lex instead of G Lex and it means that the computation can get really big as we saw in the last lecture; so, that is what we are doing here. We just do we just change the order to Lex, same ideal.

(Refer Slide Time: 27:00)



```
In [5]: %%macaulay2
        G = gens gb I;
        leadTerm I

          1      7
Matrix R <--- R

| z79 yz2 y4 xz3 xyz xy3 x2 |

          1      7
Matrix R <--- R

There is  $f_3$  with  $\text{in}(f_3) = z^{79}$ , so it is  $f_3(z)$ .
```



And we asked for its; so we have seen similar example suddenly the in much higher degree and much higher large enough. I mean more elements in the Grobner basis. So, this is again similar example.

We compute the Grobner basis of I and then we ask for the leading term. So, it gives this output. So, this is the initial ideal already. I mean we see that there are 7 terms inside here and there is one of degree 79.

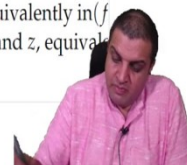
(Refer Slide Time: 27:35)



```
Matrix R <--- R

There is  $f_3$  with  $\text{in}(f_3) = z^{79}$ , so it is  $f_3(z)$ .
There is  $f_2$  with  $\text{in}(f_2) = y^4$ , so it is  $f_2(y, z)$ .
First find zeros of  $f_3(z)$ ; call them  $\{c_1, \dots, c_{79}\}$  (might be repetitions)
For each  $i$ , find zeros of  $f_2(y, c_i)$ .
This gives  $V(f_2, f_3)$ .
For each  $\{(b, c)\} \in V(f_2, f_3)$ , find zeros of  $g(x, b, c)$  as  $g$  takes the values of  $t$ 
of  $I$ .
Note that in Lex
 $f$  is a polynomial in  $z$  if and only if  $\text{in}(f)$  is a power of  $z$ , equivalently  $\text{in}(f)$ 
 $f$  is a polynomial in  $y, z$  if and only if  $\text{in}(f)$  involves only  $y$  and  $z$ , equivalent
```

In [6]: %%macaulay2



So, let us try to understand what it says. So, there is a polynomial  $f_3$  in the ideal with  $\text{in}(f_3) = z^{79}$ . But if you have a polynomial in Lex order whose initial term is  $z^{79}$  or power of  $z$  then it cannot involve  $y$  and  $x$ . So, it must be a polynomial in  $z$  alone. There is an  $f_2$  with initial term  $y^4$ . So, it must be a polynomial with in just  $y$  and  $z$ .

So, we first can solve for this one; then for each values of the solution  $c_1, \dots, c_{79}$ . So, there might be repetitions, These are algorithmic aspects that one should worry about one has to actually compute, but at least let us have an idea how it can be done.

So, for each  $i$  we can substitute  $c_i$  inside here and solve for  $f_2(y, c_i)$ . So, this will give us the variety  $V(f_2, f_3)$ . So, instead of finding the single variable polynomials we are doing like Gaussian elimination. We first solve for the last variable and then the next one and then the next one.

So, for each  $(b, c) \in V(f_2, f_3)$  find zeros of  $g(x, b, c)$  as  $g$  takes the values in the generators.

(Refer Slide Time: 28:59)

$f$  is a polynomial in  $z$  and only if  $\text{in}(f)$  is a power of  $z$ , equivalently  $\text{in}(f)$  is a polynomial in  $y, z$  if and only if  $\text{in}(f)$  involves only  $y$  and  $z$ , equivalently

```
In [6]: %%macaulay2
        select(flatten entries G, m -> m < y)
        select(flatten entries G, m -> m < x)
```

79 78 77 76 75 74 73 72 71 70  
 $\{z^{-5z} - z + z + 5z - z - 4z - 2z + 4z - 4z +$

List

79 78 77 76 75 74 73 72 71 70  
 $\{z^{-5z} - z + z + 5z - z - 4z - 2z + 4z - 4z +$



So, here is just little bit more introduction to macaulay. So, how would we know, how would be pick out among the elements of the Grobner basis? How would be pick out those which involve only  $z$  or those which involve only  $y$  and  $z$ ? I mean how do we ask macaulay to pick it out for us?

Of course, if it is written we can glance at it and then hopefully we can pick it, but that is a little tedious. So, the observation is that  $f$  is a polynomial in  $z$  if and only if  $\text{in}(f)$  is a power of  $z$  and that is true if and only if  $\text{in}(f) < y$ .

(Refer Slide Time: 29:30)

is gives  $v(2,3)$ .  
 each  $\{(b,c)\} \in V(f_2, f_3)$ , find zeros of  $g(x,b,c)$  as  $g$  takes the values of the given  
 te that in Lex  
 is a polynomial in  $z$  if and only if  $\text{in}(f)$  is a power of  $z$ , equivalently  $\text{in}(f) < y$ .  
 is a polynomial in  $y, z$  if and only if  $\text{in}(f)$  involves only  $y$  and  $z$ , equivalently  $\text{in}(f)$   
 l: `%%macaulay2`  
`select(flatten entries G, m -> m < y)`  
`select(flatten entries G, m -> m < x)`  
 78 77 76 75 74 73 72 71 70 69  
 $- 5z - z + z + 5z - z - 4z - 2z + 4z - 4z + 3z -$



So, that is what we have asked here. So, this is something called select command.

(Refer Slide Time: 29:41)

79 78 77 76 75 74 73 72 71 70  
 $\{z - 5z - z + z + 5z - z - 4z - 2z + 4z - 4z +$   
 List  
 79 78 77 76 75 74 73 72 71 70  
 $\{z - 5z - z + z + 5z - z - 4z - 2z + 4z - 4z +$   
 List  
 Exercise: read the help for the select command.





And the exercise is open a macaulay session and read the select command help for it and understand how it is done. That is the exercise. So, I ask, so it is probably clear from the context.

Consider the function which takes the Boolean value  $m$ . So, this is a monomial, I am already using that inside here. So,  $\text{lt}(m) < y$ . But  $\text{lt}(m)$  is the largest, so every term is less than  $y$ .

So, to be correct I should have written lead term of  $m$  is less than  $y$ . So, I am asking I am giving a function from this set, so this is the Grobner basis, from this set I am asking consider function  $m$  goes to or  $m$  maps to the Boolean value true or false depending on leading term of  $m$  is less than  $y$ . So, this command picks out all the elements in  $G$ . So,  $G$  itself is a matrix, so in order to get it as a list we have to do these commands. So, please look at its help.

Apply this Boolean function, Boolean valued function and pick out the ones that are true for which the output is true that is what select us. And similarly, here I pick the ones whose leading term is strictly less than  $x$  which means the ones that involve  $y$  and  $z$  only. And then, it will give us two lists and then we can programmatically try to solve them. Of course, we have not discussed any we have to solve single variable, very high degree polynomials that also one has to be able to solve. I mean if everyone like this one there is just a single polynomial. How do we find solutions of this is a different problem which we have not discussed.

So, this is the end of this section about finiteness of solution set. And in the next lecture, we will use elimination we will discuss elimination of variables as we already saw a little bit here.