

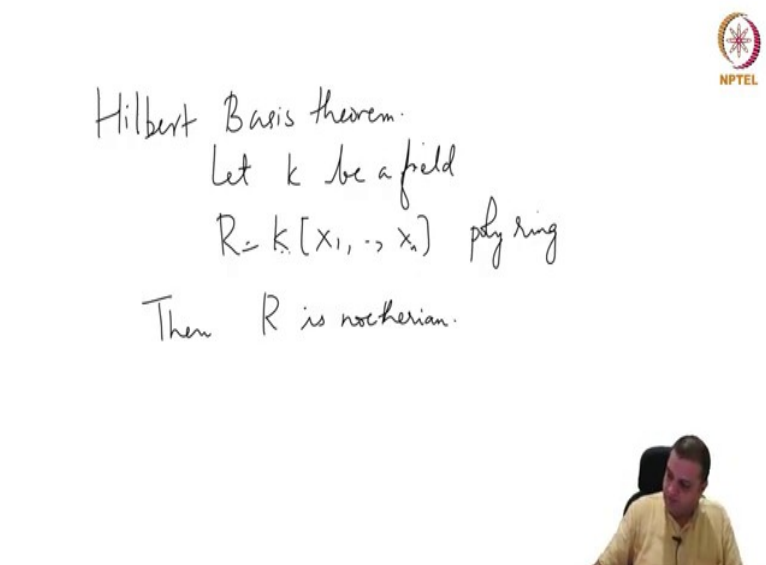
Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute

Lecture – 05
Monomials

(Refer Slide Time: 00:16)



(Refer Slide Time: 00:29)



Welcome, this is the 5th lecture in the series Computational Commutative Algebra and we start off from where we stopped last time, which was that we want to prove the following

version of Hilbert Basis theorem which is; let k be a field and R polynomial ring over k then R is Noetherian.

And as we said last time; it is not necessary to put a field here, one can take any Noetherian ring. But we will as I mentioned in order to familiarize ourselves with some tools about computational, techniques; we will restrict our proof to this thing. So, this is the version that we want to prove. So, I want to give a brief outline of this proof it is little long.

(Refer Slide Time: 01:44)

$R = k[X_1, \dots, X_n]$ Dickson's lemma: Let Λ be a non empty
Collection of monomials in R .
Then the set of minimal elts of Λ
by divisibility is finite
ie $\exists \Lambda_0 \subseteq \Lambda \quad |\Lambda_0| < \infty$
st $\forall m \in \Lambda, \exists m' \in \Lambda_0$
st $m' \mid m$.



So, the first outline; a first step or one of the steps is to prove what is called Dickson's lemma. So, what does this say? If Λ is a non empty collection of monomials in R .

Remember, R is the polynomial ring over k in n variables that is $R = k[X_1, \dots, X_n]$ and this notation is going to be used in this lecture and the next while we are discussing the proof of this theorem; monomials in R , then; sorry maybe I should just say that Λ be a non empty collection of monomials in R . Then the set of minimal elements in Λ by divisibility is finite.

What does that mean? That is, there exists a finite subset Λ_0 of Λ ; such that for all $m \in \Lambda$ there exist an $m' \in \Lambda_0$ such that m' divides m . So these are monomials in the variables X_1, \dots, X_n . So, under divisibility the set of monomials is a partial order. I mean there are pairs of monomials where neither would divide the other. So, it is not a total order and divisibility gives an order. So, this gives a partial order. So, in any non empty collection of monomials; the set of minimal elements is finite. So, this is Dickson's lemma and we will prove this.

(Refer Slide Time: 04:15)



· Every monomial ideal of R is f.g.
· monomial orders, initial terms,
initial ideals.
 $I \rightsquigarrow \text{in}(I)$ f.g.
monomial ideal
 $\Rightarrow I$ f.g.



So, using Dickson's lemma; one will show that every monomial ideal of R is finitely generated. We want to put that every ideal is finitely generated; at least we get a class where all of them are finitely generated.

The next step is to convert the problem about an arbitrary ideal to a monomial ideal. For this, we have to discuss what is called monomial orders, initial terms and initial ideals. So, given an arbitrary ideal; we will construct what is called an initial ideal of I , which should be a monomial ideal.


So, this is the strategy. I will explain the notation once we get this far, but let us just say all that one needs to know at this point is that this is a monomial ideal.

And this is finitely generated because any; every monomial ideal is finitely generated. Hence, and then we will argue that this will imply that I is finitely generated. So, this is extremely vague outline and so first we will prove Dickson's lemma and so let me just read the Dickson's lemma again.

So, let Λ be a non empty collection of monomials in R ; R is a polynomial ring that is $k[X_1, \dots, X_n]$. And the divisibility of monomials give a partial order on the set of monomials and ends also on Λ and the set of minimal elements of Λ is under divisibility ordered by divisibility is finite.

So, there exist a $\Lambda_0 \subseteq \Lambda$ which is finite such that for every $m \in \Lambda$, there exist an $m' \in \Lambda_0$ which divides m . So, let us prove Dickson's lemma.

(Refer Slide Time: 06:43)



Proof of Dickson's Lemma
Induct on n
 $n=1$ $R = k[X_1]$
 $\Lambda = \{X_1^{a_1}, X_1^{a_2}, \dots\}$
 Why $a_1 < a_2 < a_3 \dots$
 $\Lambda_0 = \{X_1^{a_1}\} \quad X_1^{a_1} \mid X_1^{a_j} \quad \forall j \geq 1$

So, this is induct on n ; if n is 1, so then R is just $k[X_1]$ and Λ is going to be just it is a set of monomial; so it is going to be powers of X_1 . So $\Lambda = \{X_1^{a_1}, X_1^{a_2}, \dots\}$ without loss of generality, we can assume that $a_1 < a_2 < a_3 < \dots$.

So, in then we take $\Lambda_0 = \{X_1^{a_1}\}$, note that $X_1^{a_1} \mid X_1^{a_j}$ for every $j \geq 1$. So this solves the problem in one variable.

(Refer Slide Time: 07:58)

$n > 1$. Assume that DL holds for $S = k[X_1, \dots, X_{n-1}]$.



Let $\Lambda' = \left\{ \mu \text{ monomial in } S \mid \exists j \text{ st } \mu X_n^j \in \Lambda \right\}$

Let $J = \{\mu_1, \dots, \mu_r\}$ be the minimal elts of Λ' . (induction)

$\forall 1 \leq i \leq r$, let j_i be st $\mu_i X_n^{j_i} \in \Lambda$



So, now let us assume that $n > 1$ and assume that Dickson's lemma holds for S which is the polynomial ring in the first $n-1$ variables that is $S = k[X_1, \dots, X_{n-1}]$.

So, now we are given this Λ ; so, now let us construct a family a collection of monomials inside S . So, Λ' be the set of monomial μ in S , such that there exists j such that $\mu X_n^j \in \Lambda$; so μ involves only the first n minus 1 variables.

So, we are doing some sort of a projection to the first $n-1$ coordinates in; we can visualize it that way if you want. So, now this is a collection of monomials in S ; it has fewer number of variables. So, Dickson's lemma applies and this now if; so let J be the set of minimal elements in this and it is a finite set. Let us call these things $J = \{\mu_1, \mu_2, \dots, \mu_r\}$ be the minimal elements of Λ' ; so this is induction.

So, for all $1 \leq i \leq r$, let j_i be such that $\mu_i X_n^{j_i} \in \Lambda$. Remember, μ_i are elements of Λ' ; so that, by that they must exist for each i ; there must exist a j_i with this property. So, this is the collection that we want.

(Refer Slide Time: 10:26)



$$\text{Let } t = \max_{1 \leq i \leq r} j_i$$

$\forall 0 \leq i \leq t$, let J_i be the set of
minimal elts of
 $\{\mu \text{ monomial in } S \mid \mu x_n^i \in \Lambda\}$
 $|J_i| < \infty$ by induction.



Let $t = \max \{j_i \mid 1 \leq i \leq r\}$. Now, for each $0 \leq i \leq t$, let J_i be the set of minimal elements of the following set which is $\{\mu \text{ monomial in } S \mid \mu x_n^i \in \Lambda\}$.

So, we have fixed an i here and then look at all monomials μ with that power of X_n . So this is a collection of monomials in S ; again by induction, it has a finite set. So, now to finish the proof; it suffices to prove the following.

(Refer Slide Time: 11:55)



$$\text{E.T.S.T } \forall m \in \Lambda, \exists m' \text{ in } t$$

$$\left\{ \mu_1 x_n^{j_1}, \mu_2 x_n^{j_2}, \dots, \mu_n x_n^{j_n} \right\} \cup \bigcup_{i=0}^t \{ \mu x_n^i \mid \mu \in J_i \}$$

(finite set)

st $m' \mid m$.

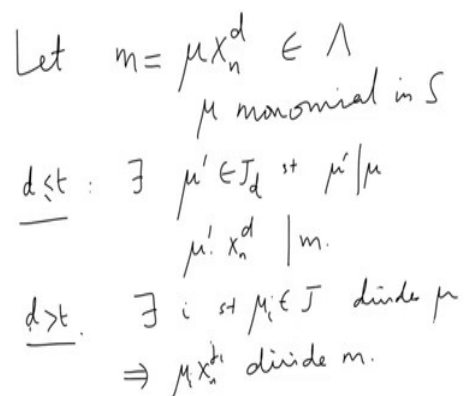
not necessarily
the set
of minimal
elts



Enough to show that; for all $m \in \Lambda$, there exist some m' in the set $\{\mu_1 X_n^{j_1}, \mu_2 X_n^{j_2}, \dots, \mu_n X_n^{j_n} \cup \{0\} \cup \{\mu X_n^i \vee \mu \in J_i\}\}$ such that $m' \vee m$.

This set is not necessarily the set of minimal elements. But the minimal elements will definitely come from this, so the set of minimal elements is finite. I mean in other words, we may have picked more elements in this set than necessary, but that is ; we just want to prove that there exists a finite set.

(Refer Slide Time: 13:53)



Let $m = \mu X_n^d \in \Lambda$
 μ monomial in S

$d \leq t$: $\exists \mu' \in J_d$ st $\mu' | \mu$
 $\mu' X_n^d | m$.

$d > t$: $\exists i$ st $\mu_i \in J$ divides μ
 $\Rightarrow \mu_i X_n^{j_i}$ divides m .

So, now let us prove that statement; so let $m \in \Lambda$; so again μ is a monomial in S . So, now let us look at the degree, let us consider two cases; if $d \leq t$, then let us go back here. So we are in this set up. So, μX_n^d is in this set and J_i is the set of minimal elements.

So, something in J_i times X_n^d must divide m , there exist $\mu' \in J_d$, such that $\mu' \vee \mu$. Then $\mu' X_n^d$ which is an element in this set; for i equals d ; it will be in the set divides m . And if $d > t$; so then there is, there exists i , such that μ_i which is an element of J ; divides μ and this implies that $\mu_i X_n^{j_i}$ divides m .

So, this is going to divide m , in both these cases we have found something that divides m . So, next we will prove that monomial ideals are finitely generated; assuming this that is not very difficult proof and then we will go on to discussing monomial orders initial ideals and so on.

(Refer Slide Time: 16:25)



Corollary: Every monomial ideal of R
is f.g.

Proof: Let I be a monomial ideal
 \exists a generating set $G \subseteq I$
consisting of monomials.



So, we now look at a corollary of the previous result Dickson's lemma; so the corollaries is the following; every monomial ideal of R is finitely generated. Remember, f.g. is for finitely generated and the proof is in immediate comes; follows immediately from Dickson's lemma that I be a monomial ideal. So, what does that mean? It means that there exist a generating set; $G \subseteq U$ consisting of monomials.

(Refer Slide Time: 17:41)



By Dickson's Lemma.
 \exists a finite subset $G_0 \subseteq G$
st $\forall m \in G, \exists m' \in G_0$ st $m' \vee m$.
Let $f \in I$. $f = \sum_{g \in G} r_i g_i = \sum_{g \in G_0} r_i g_i$
 I is generated by G_0 .

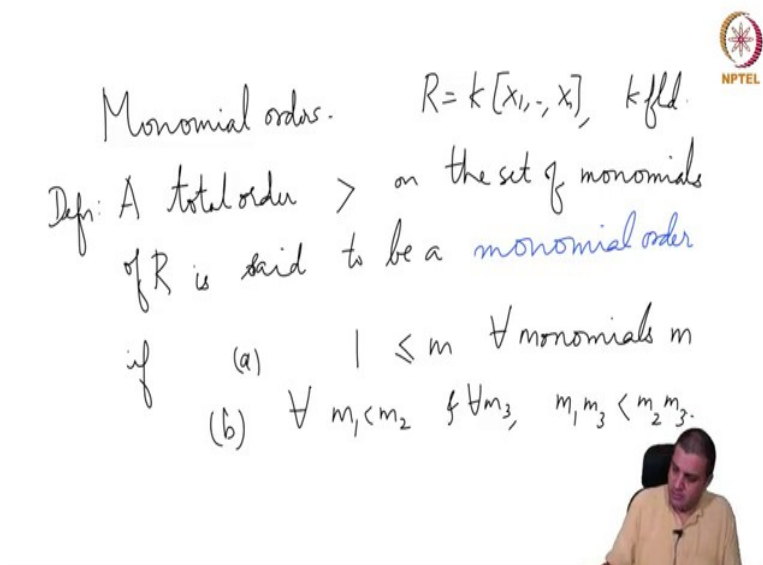


So, by Dickson's lemma; there exists a finite subset; $G_0 \subseteq G$, such that for all monomials $m \in G$, there exists a monomial $m' \in G_0$ such that $m' \vee m$.

So, now let $f \in I$, then we can write f as $f = \sum_{g_i \in G} r_i g_i = \sum_{g_i \in G_0} r_i g_i$ where this $g_i \in G$, but each of them are monomials; so each g_i is divisible by some g'_i which is inside G_0 .

So, in other words; I is generated by G_0 . So, the next step in the proof of Hilbert basis theorem, in the approach that we were using is a way to reduce an arbitrary ideal in the polynomial ring, to a monomial ideal in that polynomial ring right; so this is the idea behind it.

(Refer Slide Time: 19:36)



Monomial orders. $R = k[x_1, \dots, x_n]$, k f.f.d.

Defn: A total order $>$ on the set of monomials of R is said to be a **monomial order** if

(a) $1 \leq m \quad \forall \text{ monomials } m$

(b) $\forall m_1 < m_2 \quad \forall m_3, \quad m_1 m_3 < m_2 m_3.$

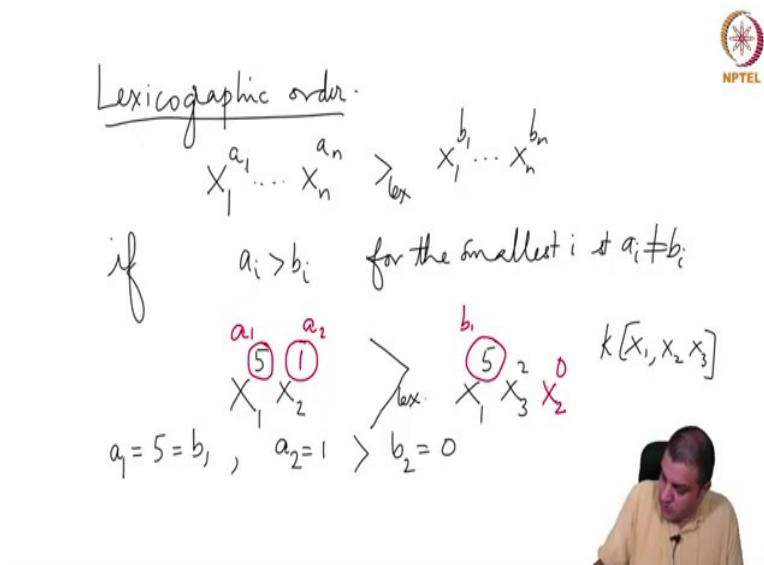
So remember that we are using a somewhat long proof of Hilbert basis theorem, so that we can introduce these notions that are relevant to computational aspects. Otherwise, we could have just proved it in more directly and a slightly general version. So, a total order; so this is the definition which we will denote by greater than symbol; on the set of monomials of R .

So, just to remind ourselves; R is a polynomial ring, in some number of finite number of variables and over a field; A total order $>$ is said to be monomial order or monomial ordering, if two conditions are satisfied: (a) the monomial 1 which is just $X_1^0 X_2^0 \dots X_n^0$, this is less than or equal to m for all monomials m .

And of course, if m is different from 1, this is a strict inequality and (b) this order respects multiplication of monomials that is for all, $m_1 < m_2$ and for all m_3 , $m_1 m_3 < m_2 m_3$. So, this is what a monomial ordering or monomial order means on the polynomial ring. So, we will look

at two examples; in fact, the second one is a variation of the first and I will put a few others in the exercises.

(Refer Slide Time: 22:05)



The slide features handwritten notes on a white background. At the top right is the NPTEL logo. The main text is written in black ink. It starts with the title 'Lexicographic order' underlined. Below it, a general comparison is shown: $X_1^{a_1} \dots X_n^{a_n} >_{\text{lex}} X_1^{b_1} \dots X_n^{b_n}$. This is followed by the condition 'if $a_i > b_i$ for the smallest i s.t. $a_i \neq b_i$ '. A specific example is then provided: $X_1^5 X_2^1 >_{\text{lex}} X_1^5 X_3^2 X_2^0$. The exponents 5, 1, and 0 are circled in red. Below the example, the text ' $a_1 = 5 = b_1, a_2 = 1 > b_2 = 0$ ' is written. To the right of the example, the polynomial ring $k[X_1, X_2, X_3]$ is noted. In the bottom right corner, there is a small video inset showing a man in a yellow shirt.

So, the first example that we want to look at is what is called lexicographic order. So, here; so we have to define what the total order is. So this is the definition; so this is a monomial with exponents and I will put a subscript lex to denote that we are referring; we are defining the lex order, $X_1^{a_1} X_2^{a_2} \dots X_n^{a_n} >_{\text{lex}} X_1^{b_1} X_2^{b_2} \dots X_n^{b_n}$ if $a_i > b_i$ for the smallest i such that $a_i \neq b_i$.

So, let us look at a quick example; $X_1^5 X_2$ and $X_1^5 X_3^2$. So, we can think of this as in the polynomial ring in three variables. So, now let us look at the exponents, these exponents we will call a_i and these exponents we will call b_i . So, a_1 is 5; which is same thing as b_1 ; so this is not 1 that is not the first time will they differ. Then a_2 is 1 and here there is no b_2 ; so this is really X_2^0 . So $b_2 = 0$.

Thus $a_2 > b_2$. So, the first index where it differs is 2 and at that point a_2 is bigger than b_2 . So, therefore the; the condition, the relation is this is bigger than this in the lex order.

(Refer Slide Time: 24:54)



In other words,
in $(a_1, \dots, a_n) - (b_1, \dots, b_n) \in \mathbb{Z}^n$
the leftmost nonzero entry is
positive.

Rmk: $X_1 >_{\text{lex}} m \quad \forall m \text{ that does not}$
involve X_1

So, in other words one can also view it as follows in other words . If you consider the following two elements in \mathbb{Z}^n and you take the difference, the exponent vector.

In this exponent vector, once you take the difference; it would be in \mathbb{Z}^n ; not the individual elements are non negative integers, but the difference could have negative entries. So, in this; the leftmost nonzero entry is positive; so that is one another way of thinking about lex order, it is just restating what we said earlier and here is a curiosity X_1 is bigger than any monomial here.

So this is really a remark; X_1 is bigger than any monomial m , for all m that does not involve X_1 . If m is a monomial in X_2 through X_n ; then that is always less than X_1 ; in fact, we can put any power of X_1 also it will be true. So, this is just to get to; I mean understand why this is true just to get used to thinking about these things.

(Refer Slide Time: 26:53)



Graded (Degree) Lexicographic order

$$X_1^{a_1} \dots X_n^{a_n} >_{\text{Glex}} X_1^{b_1} \dots X_n^{b_n}$$

if $\deg(X_1^{a_1} \dots X_n^{a_n}) = \sum a_i > \sum b_i = \deg(X_1^{b_1} \dots X_n^{b_n})$

OR

$$\left[\deg(X_1^{a_1} \dots X_n^{a_n}) = \deg(X_1^{b_1} \dots X_n^{b_n}) \text{ AND } X_1^{a_1} \dots X_n^{a_n} >_{\text{lex}} X_1^{b_1} \dots X_n^{b_n} \right]$$

So, let us look at slightly related thing; related a monomial order called graded or sometimes called degree lexicographic order. So, in the exercises, you will work out small problems to understand why the word lexicographic comes in this.

So, now let us define a similar way we have to take two monomials; $X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$ and so, we will write G lex for this thing; to say graded lex and because that is the same symbol that, that is the same phrase that Macaulay to uses; so we will try to be consistent with that. if we first compare the degrees and the one that have higher degree wins and the degrees are same, then we use ordinary lex; so, this is how it would be done.

If the degree of the monomial is; so this degree is the usual degree variables have degree 1. So $X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$, take the sum and this is greater than the degree of degree of $X_1^{b_1} X_2^{b_2} \dots X_n^{b_n}$; so that is the first condition or first check.

If this is true, then we define this to be greater in the lexicographic order or the degrees are same; meaning the sum of the a_i 's is equal to the sum of the b_i 's and so this whole thing; AND apply system, this AND; so they have the same degree and this one is the usual lexicographic order; this is bigger than that. So, let us just compare it I mean just take one example .

(Refer Slide Time: 29:35)



$$\begin{array}{ccc} X_1 & >_{\text{lex}} & X_2^2 \\ X_2^2 & >_{\text{Glex}} & X_1 \end{array}$$

Graded Reverse Lexicographic order
— Exercises —



So, let us look at this. So, if you look at X_1 and X_2^2 ; we observed earlier that X_1 is bigger than any monomial that does not involve; bigger in the lex order than any monomial that does not involve X_1 , so this is the relation between them. But, however when we do graded lex; then this has a higher degree. So, then X_2^2 is higher in the graded lex than X_1 . So, let us look at how this is done in Macaulay.

(Refer Slide Time: 30:15)



M2_01_Lex.png

```
i1 : R = QQ[X,Y,Z, MonomialOrder => Lex];  
i2 : X + Y^2  
o2 = X + Y^2
```



So, here; we define a polynomial ring in three variables, but although in the example, I used only two; R is a polynomial ring over the rationals in three variables X , Y and Z . So, what is

X_1, X_2, X_3 ? Well, X_1, X_2, X_3 are in the same order X_1 is X , X_2 is Y and X_3 is Z ; so it is in that order. And we specify that, we specify the monomial order like this; we write monomial order and then equal to and a greater than sign which is read as gets.

So, this is what is called an option to this command, this is ring construction command. So, monomial order gets the value lex; so polynomial ring $Q[X, Y, Z]$ monomial order gets lex. So, this is how what is called options are specified and then we just ask $X + Y^2$ and it just writes $X + Y^2$.

So, what information can we get from this? Well, the way polynomials will be written in Macaulay is in the decreasing order in the monomial order of the ring. So, $X + Y^2$ is written as $X + Y^2$ because X is bigger than Y^2 in lex order.

(Refer Slide Time: 31:46)



So, now yeah; so now let us look at a graded lex. So, we specify the same, same thing; except monomial order gets the value GLex; so that is the term to specify that we want graded lex. And then we enter the same polynomial $X + Y^2$, but it tells us $Y^2 + X$ because Y^2 is bigger than X in the graded lex order. So, the way the polynomials are printed itself will tell us what the leading term of the initial term.

Well, the largest term in that monomial is; it largest term in that polynomial is. So, just one more; one more order what is called graded, this is an; is an extremely important for various computational purposes and also for, it has much nice of different properties in lex. So,

graded reverse lexicographic order ; which we will do in the exercises . So, that is the; so this is the end of the 5th lecture.