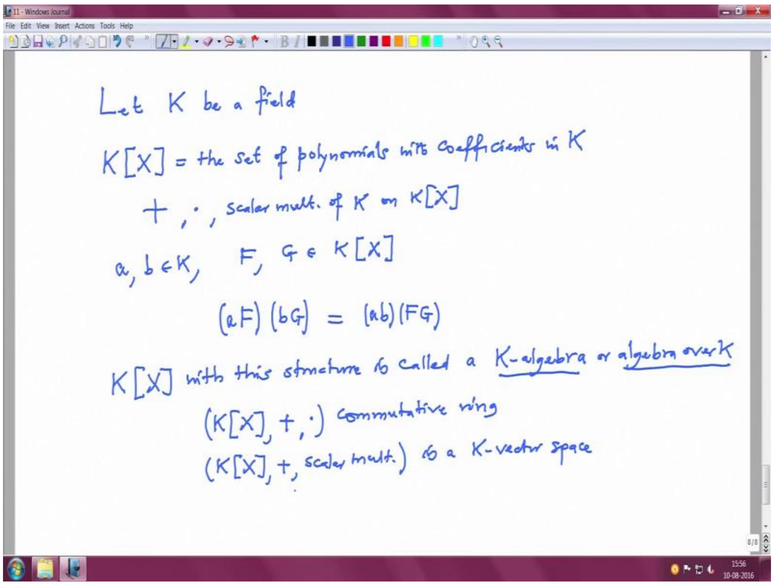
Linear Algebra
Prof. Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore

Lecture – 12
Review of univariate polynomials

Come back to these lectures on Linear Algebra. Let me recapitulate what we did in the last lecture.

(Refer Slide Time: 00:32)

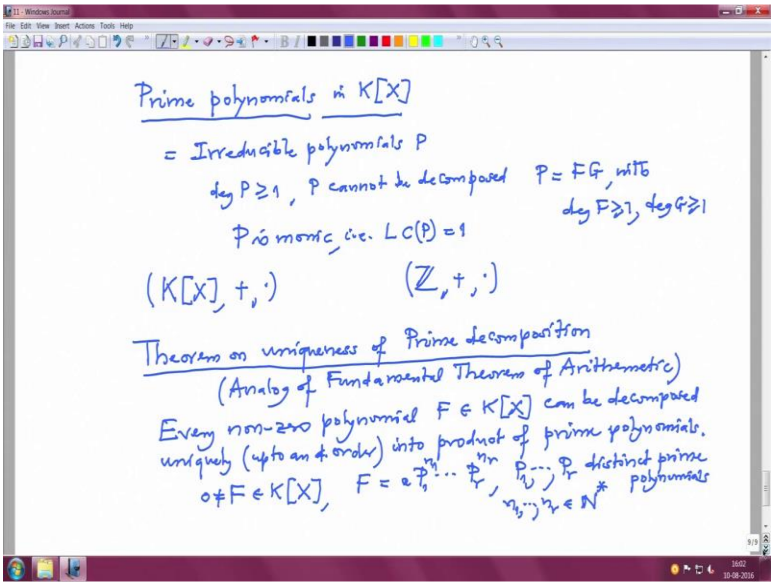


Let K be a field on the set of polynomials K X that we denoting this; this is the set of polynomials with coefficients in K we have defined operations addition of polynomials multiplication of polynomials and also scalar multiplication of K on the polynomials K X and note that we have mention that I mention that this operations are compatible with each other especially I want to note the scalar multiplication and multiplication of a polynomial.

So that means, the compatibility of these 2 operation means given 2 scalars a b and 2 polynomials F coma G in K X whether you multiply first a scalar and a polynomial, a F and b time G. So, you get polynomials and now you multiply this 2 polynomials, on the other hand you first multiply the scalars and then multiply this scalar to the polynomial; product polynomial. So, this operation should be same, this result should be same that is the compatibility of scalar multiplication of K on K X and the multiplication of polynomials. So, such a total structure these structure K X; K X with this structure is called K algebra or algebra over K.

Note that, this means you have 2 separate 2 things together that is K X with plus and multiplication of polynomials this is a commutative ring and a K X with addition of polynomials and the scalar multiplication it is a K vector space and these 2 structure are compatible and the compatibility just means this scalar multiplication is compatible with plus and scalar multiplication is also compatibility with the multiplication of polynomials and this addition in these vector space and addition in this ring are same. So, all these together are encoded in one word in that it is a K algebra.

(Refer Slide Time: 04:43)



So, further I have also discuss about prime polynomials prime polynomials are in K X are the polynomials these are irreducible polynomials.

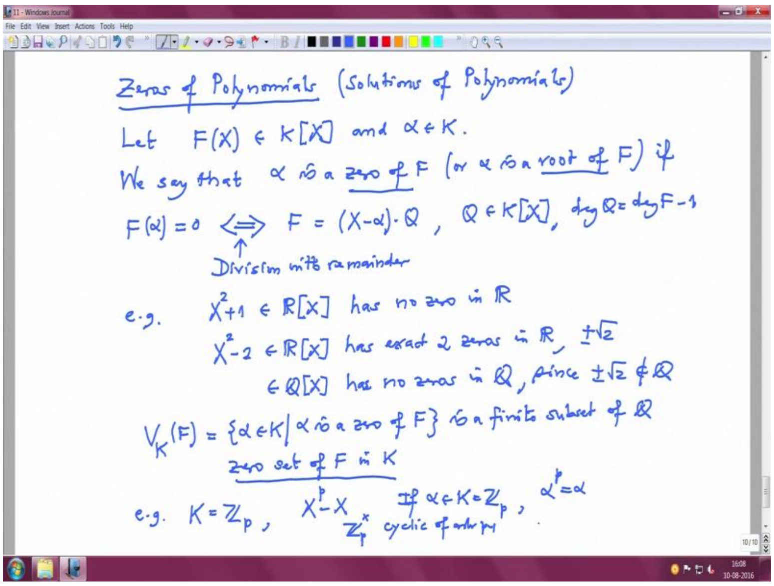
Irreducible polynomials are by definition they are non-constant polynomials that is degree of P is bigger equal to 1 and P cannot be decompose as product of 2 non-constant polynomials F G both non-constant with degree F bigger equal to 1 and degree G also bigger equal to 1, you cannot decompose these into the product and in addition to that P is monic means that is the leading coefficient leading coefficient of P is 1 these polynomials are called such polynomials are called prime polynomials and they have the same role like prime numbers and understanding the prime polynomials over and arbitrary field is a complicated problem.

However, one can describe them for special fields like complex numbers real numbers etcetera, but I will continue little bit more. So, the importance you; so, this algebra K X this ring; the ring this has similar exactly similar to that of ring of integers. So, we have seen the analog of prime numbers or prime polynomials also division with reminder also it in linear algorithm and so on. So, in addition to that I also would like to note this theorem on this is a theorem on uniqueness of prime decomposition such a theorem we know such a theorem we know such a theorem holds for integers and that theorem was called fundament theorem of arithmetic.

In this case this is the analog of fundamental theorem of arithmetic. So, it has a existence part and uniqueness part. So, existence part is simple that any even uniqueness part is simple. So, this theorem says that every nonzero polynomial F in K X can be decompose uniquely. So, when one say is uniquely; that means, up to an order decompose uniquely into product of prime polynomials in the notation if F is nonzero polynomial in K X then you can write F as some constant times P q n q P r n r where P 1 to P r are distinct prime polynomials and n 1 to n r are nonzero natural numbers they are called the multiplicities of those prime factors.

So, this is the same analog of the fundamental theorem of arithmetic to this ring this will be use quite often later in some discussion now I first I should give some examples.

(Refer Slide Time: 10:36)



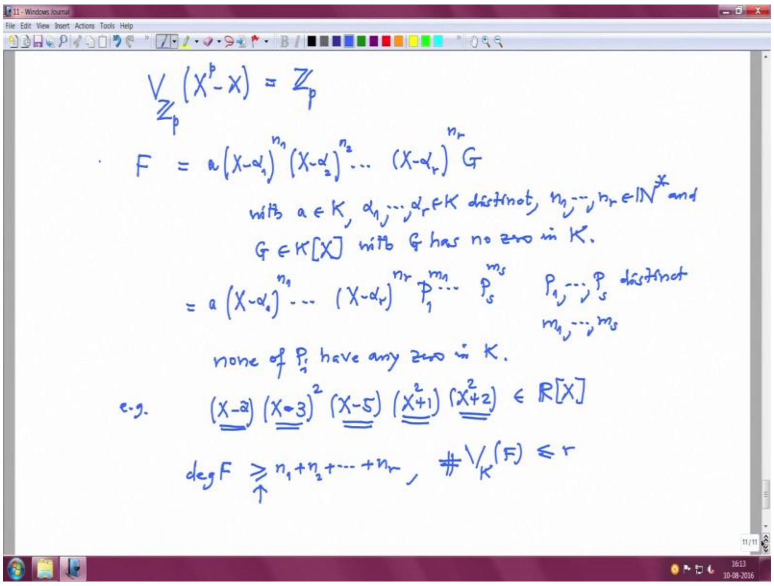
So, for example, now let I need couple of definition. So, first let me give couple of definitions. So, this is 0s of polynomials also one can call them as solutions of polynomials. So, like we have seen in earlier lecture linear polynomial solution space like that now we are considering arbitrary polynomial, but only one variable. So, let F X be a polynomial with coefficients in the field K and alpha be an element in K we say that alpha is a 0 of F or some people say or alpha is a route of if when you substitute X equal to alpha F of alpha it should become 0.

So, I would therefore, like to stick to this 0 of this terminology rather than the route this is equivalent to saying F is a F can be written as a product of the linear factor X minus alpha time some Q where Q is some polynomial and; obviously, the degree of Q will be exactly 1 less than the degree of F this equivalence follows immediately from the division with reminder this is for this one needs to use division with reminder. So, it polynomial with coefficients in K may have 0 in K or may not have for example, the polynomial X square plus one with real coefficients if you think them as the real coefficients then this polynomial has no 0 in real numbers whereas, if you take this polynomial X square minus 2 in real numbers has exactly 2 0s in R namely plus root and minus root 2.

Whereas, the same polynomial if you think is a polynomial in with rational coefficients then has no 0s in Q because the 0s are precisely plus minus root 2 and the they are not rational numbers because since plus minus root 2 they are not rational numbers. So, therefore, when one talks about a roots etcetera one needs to specify the field more carefully also I will introduce a notation here that V K of F this is alpha in K such that alpha is a 0 of F this is finite subset of q it could be empty also this is called the 0 set of F in K for example, in this case if you take this as a rational numbers it is an empty set if you take over real numbers it is plus minus root 2 this as a empty set and so on, one more example for finite filed now suppose we take K equal to Z mod P and the polynomial X power P minus X.

Then we know that all elements if alpha is in K; remember K is Z mod P and you know that alpha power P equal to P for all alpha because the group Z P cross the multiplicate to group of that finite field Z mod P is cyclic of order P minus 1 and so alpha power P minus 1 is always 1 and you multiply that by alpha.

(Refer Slide Time: 16:36)



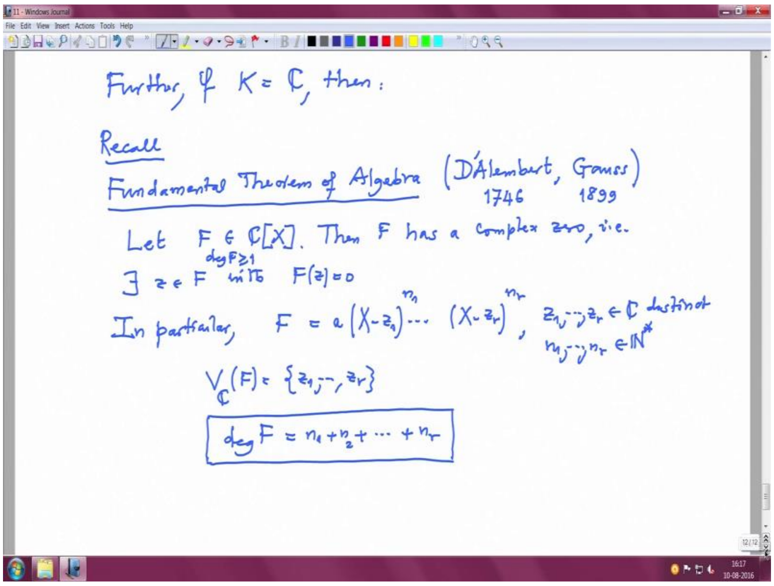
So; that means, this means the 0 set of in Z mod P 0 set of the polynomial X power P minus X is all Z mod P alright you can also do little bit finer analysis that if we have a polynomial you can try to take out all the possible 0s as a product because we have seen if alpha is a 0s and X minus alpha is a factor.

So, every polynomial F therefore, we can write it as a times X minus alpha 1 power n 1 X minus alpha 2 power n 2 and so on till X minus power X minus alpha R power n r still some polynomial part may be left who do not have 0 at all. So, that is G with first a is in scalar a is a scalar alpha 1 to alpha r are elements in K distinct n 1 to n r are the multiplicities of alpha 1 to alpha r are respectively and they are nonzero natural numbers and G is a polynomial with coefficients in K with the property that with G as no 0 in K it map and G could be prime or may not be prime if it is not prime further you can decompose into the prime factors, but those prime factors will also not have any 0s in the field K.

So, in any case we can also write this as this product as it is and then further write G as a product of prime polynomial this is m 1 P s m s where P 1 to P s are distinct prime polynomials and m one to m s are there multiplicities in F and P i any no none of the P i is have any 0 in K for example, just one could write easy example one could write an example like this if you look at X minus alpha X minus let us say 2 power 1 minus 3 square X minus 5 then X square plus 1 X square plus 2. This is think of this is a polynomial with real coefficients this guys are corresponding to the 0s 2 3 5 the multiplicity of the 0 2 is 1 multiplicities of the 0 3 is 5 multiplies of 5 is one these are prime factors because this polynomials cannot be further decomposed into 2 linear once because minus does not have square root in real numbers negative numbers have no square root.

Therefore this and you can cook up any example with any configuration alright. So, in general you could also write the degree and F. So, degree of F in any case will be bigger equal to the sum n q plus n 2 plus, plus, plus, plus n r and the cardinality of the 0 set of F will be bounded by the number R. So, this R because we are counting when you count in the set 0 is counted only once, but in this product. So, this formula is finer this is finer then this inequality further if your field is better field as nice properties.

(Refer Slide Time: 21:31)

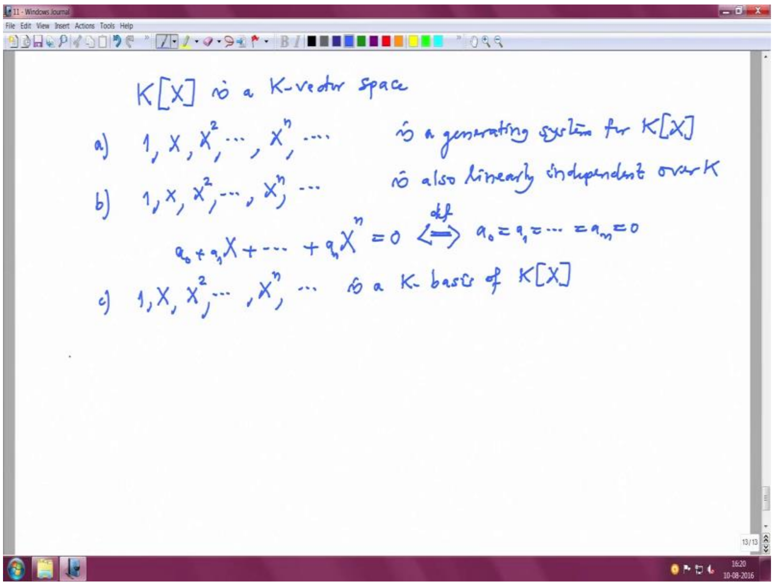


Further, if one takes K equal to E when you can of course, improve the things then we can there is no the other does not exist then I recall what is called as fundamental theorem of algebra.

This was first time stated with D'Alembert the French mathematician D'Alembert is stated this formally in 1746 and the first correct proof is due to Gauss in 1899 that was his (Refer Time: 22:44) he say that let F be a polynomial with a complex coefficients then F can be then F has a complex 0; that means, there exit a complex number Z in F with F of Z is 0 and when I say polynomial non-constant. So, that is degree F is bigger equal to 0 bigger equal to 1. So, once you do this then X minus Z will be factor of F and then the remaining part again you can apply this theorem. So, in particular we will get a decomposition like this F equal to some constant X minus Z 1 power n 1 X minus Z r power n r where Z 1 to Z r are different distinct complex numbers and n 1 to n r are the multiplicities of this 0s then nonzero natural numbers.

So, in this case V c of F is precisely Z 1 to Z r and if you count them properly then you get a nice formula that is degree F equal to n plus n 2 plus, plus, plus, plus n r otherwise you have just less equal to. So, this theorem will be often use especially in the computation of eigenvalues characteristic polynomials etcetera, etcetera and normally in courses like linear algebra one does not proof this, but assumes this. So, I am also going to assume this theorem all right. So, coming to our vector spaces this was a little bit long digration with polynomials etcetera and I will come back to it with the more force in rational functions, but I will not talk that now.

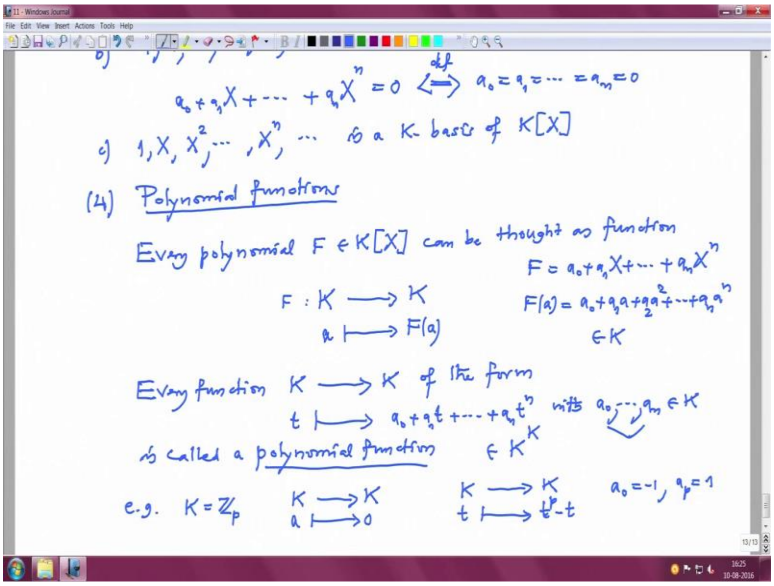
(Refer Slide Time: 25:46)



So, this was a point to give an example of a vector space and the basis generating side linear independence basis etcetera. So, this vector space K X, we have noted this K X is a K vector space; obviously, I will keep noting a b c a if you look at the family 1 X square all powers of the indeterminate and. So, on this is generating system or K X, this is obvious because we know any polynomial is a linear combination of this powers of X so, but note that this family is not finite it is a countable family, but it is not a finite b want to say that this family 1 X X square etcetera X power n etcetera, etcetera is also linearly independent over K this is again obvious because if we have a finite some like this a 0 plus a 1 X plus, plus, plus, plus, plus, plus a n power X n if this is 0; that means, this is a left hand side is a polynomial which is 0 polynomial, but; that means, by definition all these coefficients are 0 this is a definition of a polynomial.

So, put in together we know that 1 X X square etcetera this is a basis, this is a K basis of K X. So, K X needs infinite basis countable basis. So, later on when I introduce a concept of dimension we will check that the dimension of the vector space K X is countable, but these I do it in the next section, but now the next example I want to. So, I forgot the number let me check the number this is also rather long discussion on the polynomials I thought it is good idea to recall about polynomials.

(Refer Slide Time: 29:05)



So, fourth example, this is example four now this is I want to discuss polynomial functions. Note that each polynomial every polynomial F it coefficients in the field K you can think of a function can be thought as a function from where to where from K to K and that also I keep denoting by F only.

But remember when one says one has to be little careful when writing what we are talking. So, which function ant constant just substitute that constant instead of a variable F of a. So, if F where a 0 plus a 1 X etcetera, etcetera, a n X n then F of a is just putting capital X equal to small a a 0 plus a 1 a plus a 2 a square and so on, a n a power n this make sense and it is an element in K again because all coefficients where in K and we started also in a a in K. So, it is a function from K to K. So, every function from K to K of the form any, now a let me use t because t is varying in K to goes to a 0 plus a 1 t plus, plus, plus, plus a n t power n with a 0 to a n and in K.

Such a function is called polynomial function is called a polynomial function and note that this is an element in K power K in our notation I will end this first of for the lecture with the following example this is just to show you that this coefficients may not be uniquely determined. So, for example, if you take the field to be K to be equal to Z mod P and poly the 2 functions K to K and a goes to 0. This is a constant function on the other hand take the other function K to K any t goes to t power P minus P minus t and we have just seen above that every element of K t power P equal to t. So, this is indeed a 0 function. So, these 2 functions are equal.

So, in this case the coefficient where minus a 0 and the next 1 is a P which is 1. So, in this case, a 0 equal to minus 1 and a P equal to 1 and in this case, they all coefficients are 0 both are 0 functions. So, this is a different representation then this. So, this unlike polynomials the coefficients are not uniquely determined thank you. So, we will continue after a break.