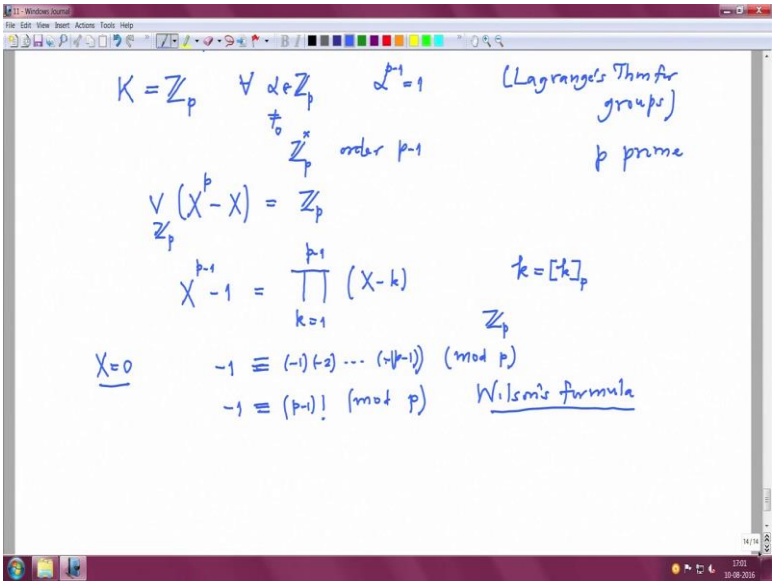
Linear Algebra
Prof. Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore

Lecture – 13
Examples of univariate polynomials and rational functions

I just want to also note two special cases of what we have discussed.

(Refer Slide Time: 00:26)



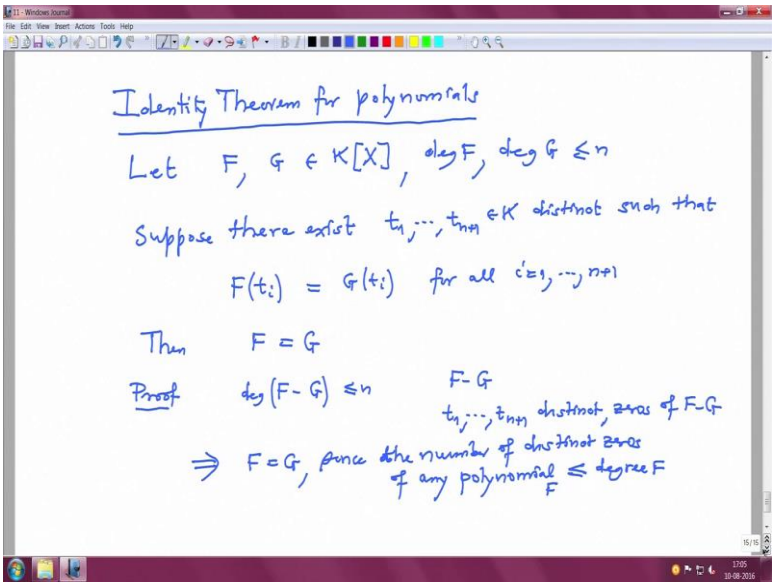
Namely; if you take the field K is Z mod p then we have said that every element alpha n Z mod p power p minus 1-th power equal to 1 that is because this alpha is in the in the alpha nonzero you alpha is in the group Z p cross this is a group and this is a group of order of this group is p minus 1 and every element raise to order of the group is identity element in that group this is Lagrange's theorem for groups therefore, every element alpha is a 0 of this polynomial likes power p minus X.

So, V Z p, I already mentioned this, but let me write once more this is all Z p in particular if you look at this polynomial X power p minus 1 minus 1, this I can factorize into linear factors Z mod p that is this will be the product X minus K, K varies from 1 to p minus 1 here this Ks, I am identifying with their equivalence classes the residue classes mod. So, in these; this is a polynomial identity with coefficients in the field Z mod p in this if I substitute X equal to 0 what do I get? I get minus 1 because this is 0 equal to this is 0 and product minus K. So, many times, so minus 1 times minus 2 go on; go until

minus p minus 1 and this is congruent to modulo; this is this equality is a congruent modulo p mod p.

This is this is something famous. So, this minus 1 coming, how many times even number of times because p is prime node p is prime number. So, this is same as minus 1 is congruent to p minus 1 factorial modulo p this is called remember this is called Wilson's formula so, which we have proved it on the either by using the polynomial identities.

(Refer Slide Time: 04:18)

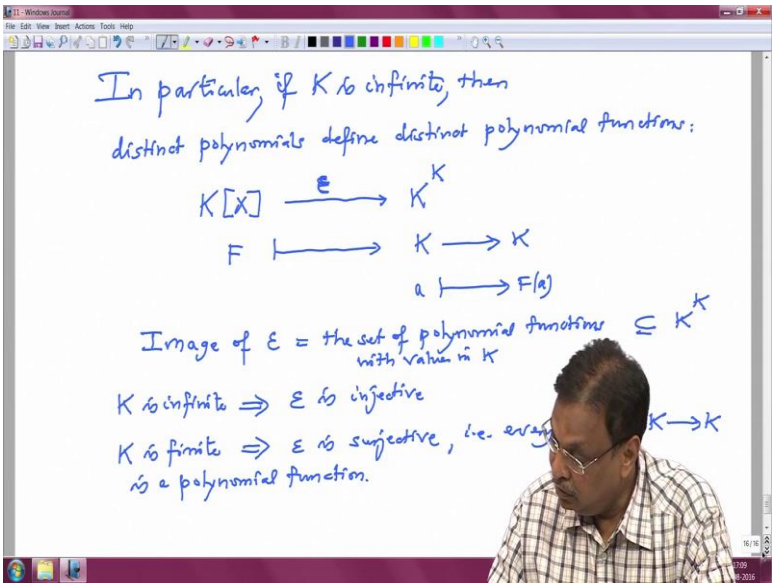


The next one, I want to mention which also we will lead to more often this is theorem on identity theorem for polynomials very useful for remaining calculations in particularly for interpolations.

So, let F and G be 2 polynomials of degree F and degree G both are less equal to n, we want to we want to know how do we infer that F equal to G the conditions to conclude F equal to G equality of G. So, the condition is suppose there exist n plus 1 different elements t 1 to t n plus 1 in K distinct elements in the field such that when I evaluated at F at t i and evaluated G at t i and if these are equal for all i from 1 to n plus 1 then already the polynomials are equal then F going to G proof just look at the difference polynomial F minus G the degree of this difference cannot exceed n because both are of degree less equal to n.

So difference will be not more than degree n, but this polynomial F minus G all these points t 1 to t n plus 1, these are distinct and the assumption the values are equal to say that they are 0s of F minus G and we know polynomial of some degree can have at most those many different 0s therefore, the only possibility F equal to G. So, I will that there is a near since a for a the number of distinct 0s of any polynomial is bounded by 2 degree F for any polynomial F the number of 0 distinct 0s of any polynomial F is less equal to the degree F here the degree is could be even smaller then n and there at least n plus 1 distinct 0.

(Refer Slide Time: 08:30)



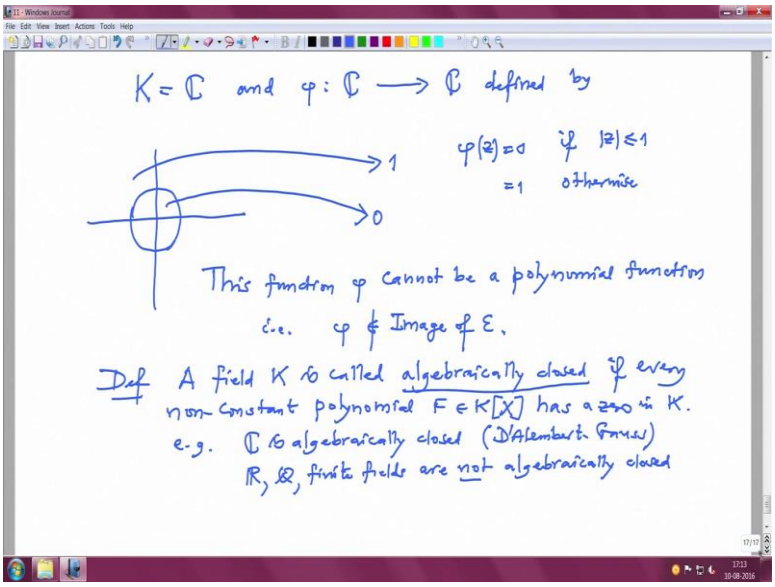
So, degree; so this is very simple. So, in particular when your field is infinite then so in particular, what is the immediate consequence of this? So, in particular if K is infinite then distinct polynomials define distinct polynomial functions you may write in the notation to for a clear understanding this mean the following see we have the set of polynomials here and we have the set of functions and we have a natural map here the map is taken E F, this is a map, I would denote by epsilon F goes to it should go to a function K to K this is the function a goes to F of a. So, polynomial has map to function this is so polynomial function.

The image of epsilon image of epsilon is precisely the set of polynomial functions with values in K epsilon in K. So, this is a sunset of this K power K, what we have approved here is if K is infinite; K is infinite then this map epsilon is injective if I have 2 different

polynomials then there images has functions are different that is because if they are equal then their function; they are equal then they will be equal at infinitely many points in particular they will be equal to more than the degree points and therefore, by earlier remark they will be equal.

Now, it is very interesting to find what is this image set in general, I will just now give only one more remark that too without proof if K is finite, this will be written more in supplement if K is finite then actually epsilon is surjective; that means, any polynomial function any function is coming from a polynomial function it is defined by polynomial function. So, this means so that is every function from K to K is a polynomial function just 1 example just to digress. So, let us take; now do not take K finite and see what happens to this surjectivity?

(Refer Slide Time: 12:30)



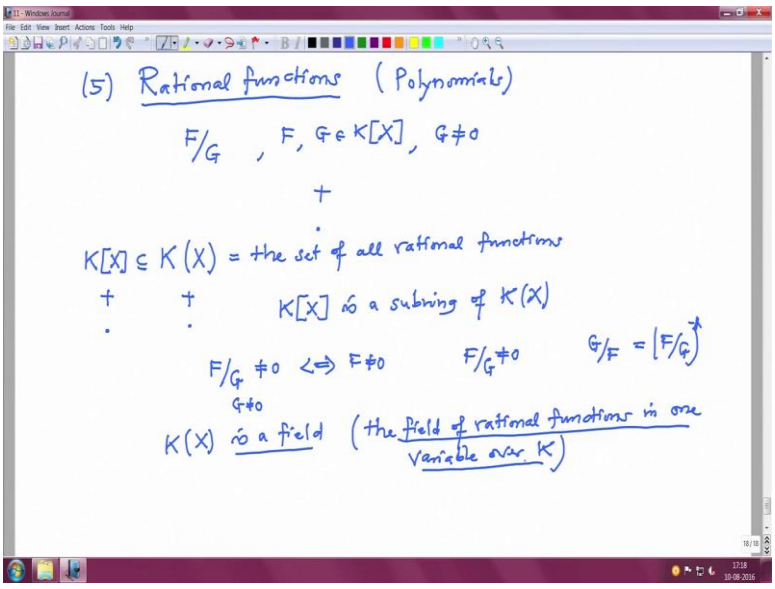
If K is C complex numbers and suppose I take a function and phi is a function from C to C. So, defined by say on the disk, this is the think of complex numbers as these complex planes on the disk on this you define it to be 0 functions and everywhere else you define it to be from value 1. So, formally writing is phi of Z with 0 if mod of Z is less equal to 1 and equal to 1 otherwise. So, you get a function from C to C this function cannot be polynomial function this function phi cannot be a polynomial function that is the function phi does not belong to this image of epsilon.

Image of epsilon is precisely the polynomial functions why that because you see the whole disk is mapped to 0 thedisk has many infinitely many complex numbers. So, if it were a polynomial function it will vanish only at in finitely many points, but this function furnishes. In fact, countable in uncountable many points, so this cannot be polynomial function, I want to end this by giving only one definition. So, this also will be very convenient to use this terminology later field K is called algebraically closed if every non constant polynomial F in K X has a 0 in K.

Once it has 1 0 then you can repeat the argument and every polynomial all the 0s will be in K this is for example, theorem of gauss D'Alembert says C is algebraically closed this is D'Alembert gauss incidentally D'Alembert wanted to proof this theorem because you wanted to solve deferential equations this, I will do it in when we do solutions of the differentially equations and on the field r q finite fields are not algebraically closed. So, proving theorems in linear algebra over C will be easier for this reason because C is algebraically closed and because the other fields are not algebraically closed the proving theorem support Eigen values etcetera.

They will be more difficult to prove, but similar techniques work for arbitrary fields now I want to continue next example also I have to finish this. So, I have to also digress about example 5, I think rational functions I will be more briefer in this.

(Refer Slide Time: 17:01)



So, the first one is I just want to define. So, rational functions are like rational numbers that is by the name rationals and still one should not call function one should actually call rational polynomials, but in the literature they are referred as rational functions. So, I will keep using, but I will warn you when some things are necessary.

So, what are rational functions they are polynomials by one polynomial by another polynomial like a fraction, one integer divided by another integer. So, F and G are 2 polynomials over a fields in one variable and G should be a nonzero polynomial and; obviously, you know you extend a definition of sum of polynomials by usual fraction there will be K in the denominators love like what do you have the need for the rational numbers and also similarly you can multiply them. So, this is multiplication of rational polynomials. So, already with this the set of all rational functions are denoted by K round bracket X this is the set of all rational functions.

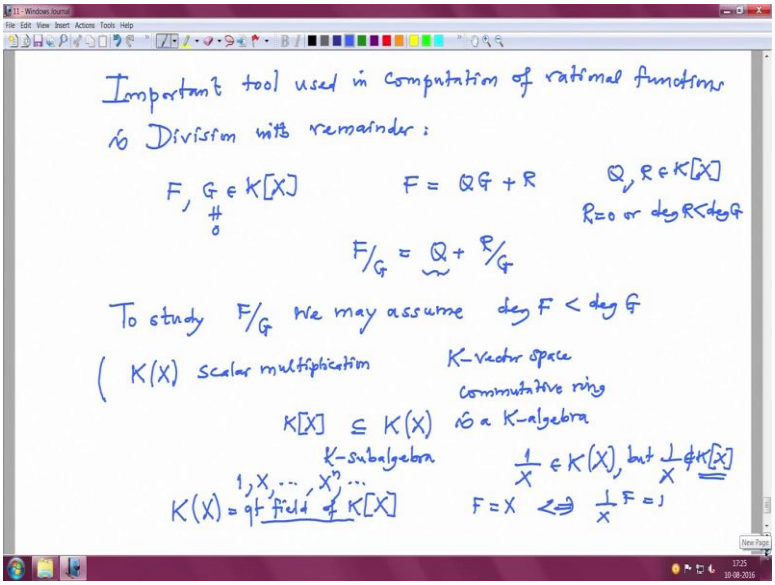
And one of the aim in this example, I want to show you this is a vector space and I want to find a basis for this vector space this is the aim of this. So, I am diagnosing which will lead us to finding a basis and that is very very important because especially if you remember how you have integrated the functions integrated rational functions there you have used a technique called partial fractions and. So, I am recalling those things in a brief way frame, but more or less self content so; obviously, all polynomials are rational functions and we have extended the definition of some of polynomials and product the polynomials to the rational functions so; that means, we have extended this ring this K X is extended to this bigger ring.

So, the binary operations are in the polynomial ring are the restrictions of the binary operations from the bigger set so; that means, this K X is a sub ring of rational functions this is also ring K rational functions with the additional multiplication is; obviously, a commutative ring say similar way you can what we have done for a polynomial you can check this is a formal checking actually it is better because any rational function if it is a nonzero rational function; nonzero simply means F is nonzero; obviously, in the in the definition G has to be nonzero, but the rational function is 0 if and only if the numerator polynomial is nonzero.

So, this means I can invert it so; that means, this F over G if it is nonzero rational functions then G over F also make sense and that is also rational function and this is the

inverse of F over G in this ring this is the inverse so; that means, we have checked that this set of rational function K round bracket X is actually a field that is a reason sometimes it is called the field of rational functions in one variable over K. So, this now we have added one more field in our list, how do you construct the bigger field from a given field.

(Refer Slide Time: 22:20)



So now the most important tool used in the calculation or in computation of rational functions is of course, division with remainder. Remember, we have we have divided if we have 2 polynomials F and G and if G were nonzero then we have divided F by G and written a quotient and remainder so; that means, you have written F as Q time G plus R where Q and R are polynomials again uniquely determined with a property that either R is 0 or degree of R is smaller than degree of G. So, the same thing now I can use it rational function and same equation I rewrite is F by G equal to Q plus R by G just divided both sides by G.

So, I want to study these rational functions F by G this is a polynomial Q is a polynomial. So, I might concentrate on the R by g. So, to study F by G we may assume degree of numerator F is strictly smaller then degree of the denominator G because I will forget this and Q is polynomial. So, we know how to study polynomials better then rational functions. So, I will just concentrate on this part and this part has numerator is degree is a really 0 its rational function 0. In that case we stop because we know we have

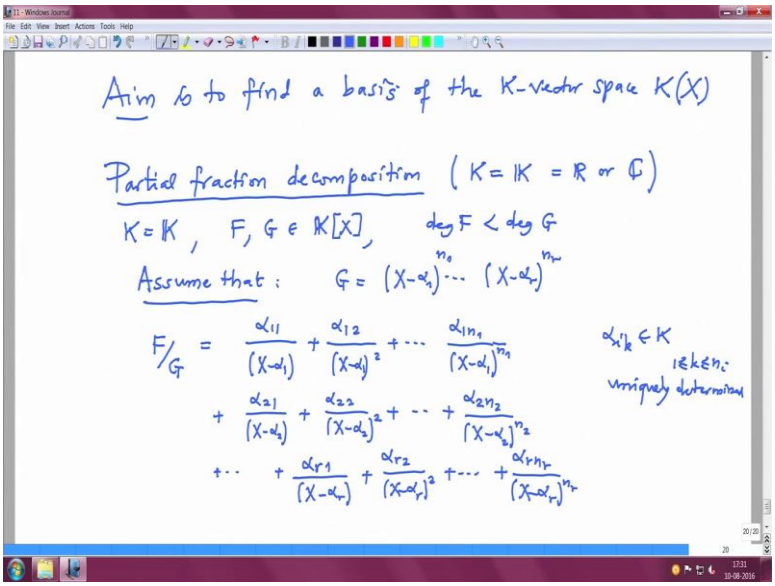
to study only polynomial. Otherwise we can assume this I forgot to mention that this rational functions also as a just scalar multiplication these are also scalar multiplication of K and again the ring structure and this scalar multiplication are compatible because that was we have checked that in polynomial case and the same checking will also check that this is compatible with the ring structure of the field of rational functions.

So, that mean this field is K vector space and also commutative ring and these structures are compatible so; that means, K rational functional field is also K algebra remember K algebra means vector space and commutative ring and both these structures are compatible and this the polynomial algebra this K algebra K X polynomial algebra is a K sub algebra of and by the earlier results and remarks we know that this the elements in this polynomial algebra are studied better and now I am I want to here we have a basis the basis here was remember 1 X powers of X this is a basis, but here we need more remember 1 over X is never polynomial 1 over X this is a rational function this is in K round bracket X, but 1 over X can never be polynomial when I X cannot be invertible in the polynomial ring.

Because you see if there is a polynomial inverse of this then you can write it 1 over X times F equal to 1 and then shift this X to the other side then you will get this is equivalent to saying F equal to X, but still what is the contradiction? So, check that this is not possible F can X cannot have inverse because inverses we have noted inverses have only degree possible degrees are 0 because of the degree formula and this degree is one. So, this cannot have inverse. So, F will not be polynomial in F will not be polynomial, but it is a rational function.

So, in the rational function something better happens now polynomials become in veritable here. So, it becomes a field in a smallest possible way. So, this means this polynomial ring you have embedded in a smallest possible way it to a this bigger field of rational functions this is also sometimes called the quotient field of K X is also called quotient field of K X more on this usually one studies in a course on algebra or algebraic geometry and things like that. So, I will not get more in to details in this, but I will do it only what we need in a linear algebra course.

(Refer Slide Time: 29:13)



So, remember our aim is to find a basis of the K vector space K X K round bracket X with a field of rational functions.

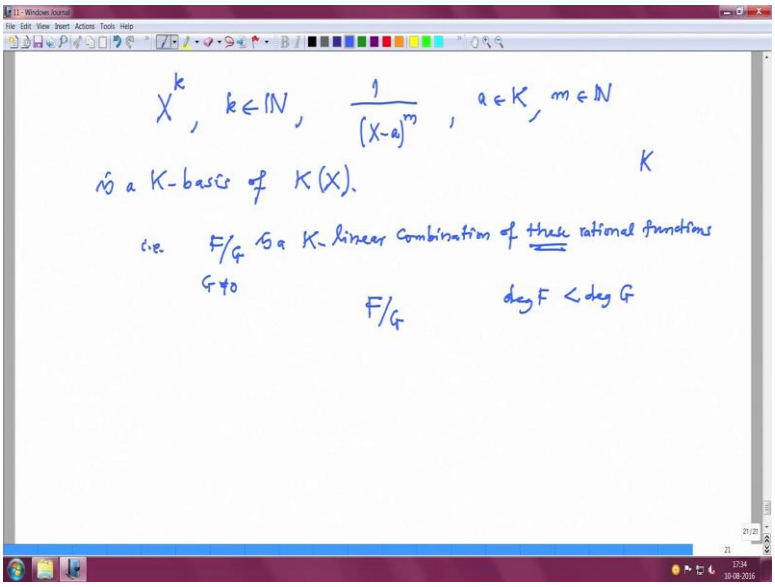
And we are going to repeatedly use the fact that we will repeatedly make use of the fact that division with remainder. So, I want to talk about first case where the denominator polynomial splits into linear factors. So, I want to recall what is the partial fraction decomposition I want to recall this I will write down the precise statement, but I do know whether I will provide a proof in this course or definitely they will the proof will be in the in the nodes and especially this is more interesting when the field is either this is the notation I will keep using this is either field of real numbers or the field of complex numbers in this case it is more important.

So, let me stick to that case. So, K is K X K is the double line k; that means, it is either field of real numbers or the field of complex numbers and let us take 2 polynomials F and G in K X and I will also assume that the degree of F is smaller than degree of G and I will also assume to start with the field is C or I will want to assume that that G is a product of linear polynomials. So, G factors like this G is X minus alpha 1 power n 1 and X minus alpha r power n r this happens for any polynomial in C that is what we have seen in the earlier part of the lecture in this case how can you write F by G that is a question F by G can be written. So, this can be written in the form alpha 1 1 divided by

X minus alpha 1 plus alpha 1 2 divided by X minus alpha 2 square go on till you achieve the full power that is alpha 1 n 1 X minus alpha 1 power n 1.

And then start with the next 0 this is done for the; this factor and alpha 2 1 divided by X minus alpha 2 plus alpha 2 2 X minus alpha 2 power 2 this is not alpha 2 this is alpha 1. So, on go till alpha 2 n 2 X minus alpha 2 n 2 and keep doing this the last will be alpha r now alpha r 1 X minus alpha r plus alpha r 2 X minus alpha r square plus, plus, plus, plus alpha r n r X minus alpha r power n r where this alpha i K they are constants this for a fixed I, this K varies from 1 to n i and they are uniquely determined I want to prove this. So, right now, we assume this and let us; let me conclude what we approved then.

(Refer Slide Time: 34:52)



So, what is it useful for? So, this means, so, what I want to claim is a fact take the powers of X K is varying from where 0 to everywhere at. So, better to write K is in n and then take such things 1 over X minus a power m now what is what is varying A is varying in the constant and this m varying as a natural number. So, I want; so what you have check that is if you take this big set this is K basis of K X because let us go back and show you. So, here if you have a; so what does it mean that you want to show it is a basis that mean you want to show that any rational function is a finite linear combination of this case.

So, that is any F over G where F at arbitrary polynomials G nonzero this should be this is linear K linear combination of these rational numbers this is small these rational

functions these special rational functions these means powers of X and this simple rational function this is 1 over X minus a power m a is varying m is varying. So, what did how do you do this first of all use divisional way some to assume that F over G as a property that the degree of this the numerator is smaller than degree of G how did we achieve that see if you go back see here you have taken the divisional of with and we look at F by G and then you get a polynomial, but polynomial vary the finite some of the X powers in a unique way.

So, this part you have managed now we have to manage this part r over g, but therefore, we have an extra assumption that degree of the numerator is smaller than degree of the denominator and now remember that I am assuming remember that I am assuming K is C in this, this is very important. So, I should write here this double K this double K right once you have assumed that then the denominator polynomial will splits into linear factors because of that assumption I can assume G factors like this and I can absorb the if G as the top degree coefficients of nonzero constant that is in a field. So, I could have absorbed that in a big numerator by multiplying by inverse.

So, without loss, I can assume G is like this and in that case what is the partial fraction decomposition says that F by G looks like this, but you see this is this is a coefficient of 1 over X minus alpha 1 this is a coefficient of 1 over X minus alpha 1 power 2 and so on. So, what this partial fraction decomposition precisely means that this rational function can be written as a finite K linear combination of this special rational functions. So, therefore, it is a basis and now this basis is bigger. So, this in and also its nice because this was the basis of the polynomial ring and this we have extended to basis. So, I think I will stop here and we will be continuing next time.

Thank you.