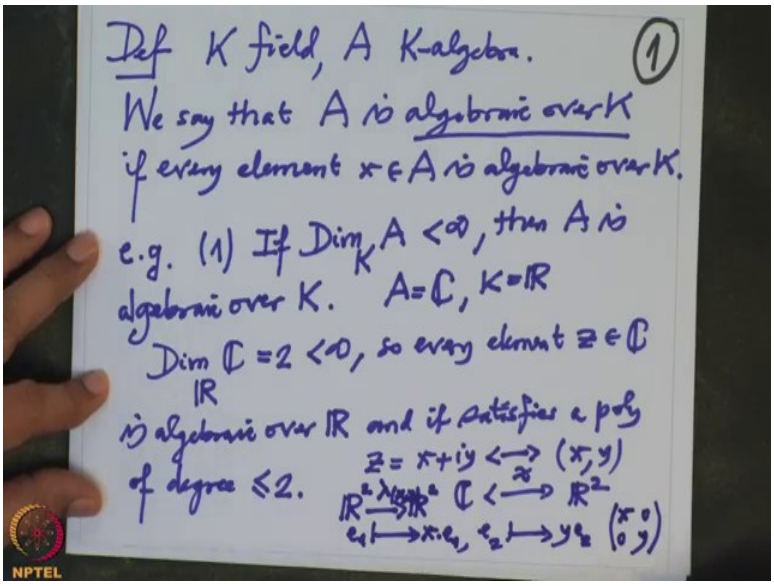
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Banglore
Lecture 16
Characterization of Algebraic Elements

Ok, so we have been debating on the concept algebraic and its minimal polynomial and so on.

(Refer Slide Time: 00:40)



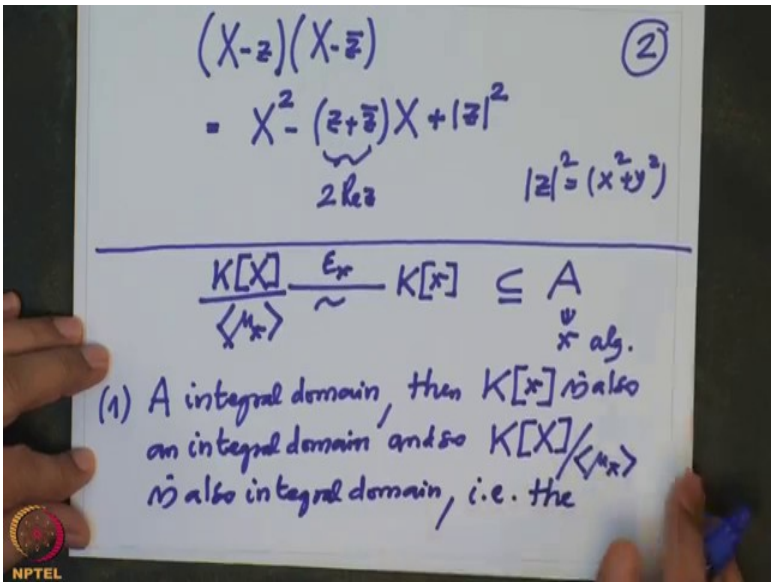
So let me formally define, suppose so definition, K field, base will be always and A K algebra we say that A is algebraic over K if every element x in A is algebraic over K that means its satisfies a non-zero polynomial with coefficients in K then such an extension is called algebraic extension. For example, we have seen already finite dimensional algebra over always algebraic, if dimension of K as a vector space over K is finite then A is algebraic over K, particular case particularly you can take A equal to let us say $\mathbb{C}$ and K equal to $\mathbb{R}$ then we know that dimension of $\mathbb{C}$ as a vector space over $\mathbb{R}$ is 2 which is finite therefore every element so every element $\mathbb{Z}$ in $\mathbb{C}$ is algebraic over K, algebraic over $\mathbb{R}$ and it satisfies (it satisfies) a polynomial of degree less equal to 2 because the dimension is at most 2.

Minimal polynomial will be bounded by the dimension of the bigger algebra. So therefore it is either a linear polynomial or quadratic polynomial. So you know how to find that as it is very

easy to find that. So suppose z is $x+iy$ then you want to find this minimal polynomial of z, so think of this x y, $x+iy$ as x, y because we have identify (identified) $\mathbb{C}$ with this real vector space of dimension 2 and this is the isomorphism between them, 1,i is the basis so that means this, so that means I want to find the minimal polynomial of this, which is like a particular case of the earlier example that means that I will do it by finding the matrix of this multiplication left multiplication by this element so that means what matrix I want to find?

That means I want to find if I take a map from $R^2 \to R^2$ this is a left multiplication by this is x, y that means e_1 goes to xe_1 and e_2 goes to ye_2 and then the matrix is what? It is clear, the matrix is x here, y here, 0 here, 0 here, then we have to find the minimal polynomial of this matrix. So and then we would get back to the identification. So check that there is a little sloppiness in this so which is better corrected like this. So, because we have identified this identification is only identification in a vector space, it is not identification as a algebra that is the sloppiness here.

(Refer Slide Time: 5:19)



So the best way to do is, so we want the real polynomial and degree with at most 2, so obviously $(X-z)$ should be a factor and the other factor will be $(X-\bar{z})$, this polynomial is $X^2-(z+\bar{z})X+|z|^2$, this is a minimal polynomial. So when this is 2 times real part of z I think

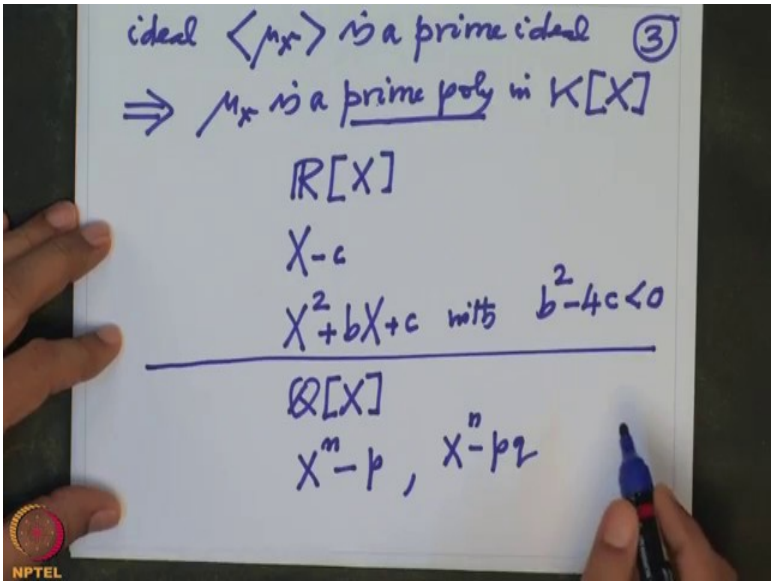
this we have argued earlier also this is the x^2+y^2 , $|z|^2$ is by definition x^2+y^2 , so this is the minimal polynomial it can thus satisfies smaller than that unless the z is already a real number and in that case it will be linear polynomial, so that is how one should try to calculate.

Now it becomes important to test how do we test an element is algebraic or not in a simpler way? That means I want to bring in more theoretical consideration to decide for example, before we don't have to check anything if I give you a finite dimensional algebra and say you check that it is algebraic. We definitely know finite dimensional algebraic is an algebraic. So now I am preparing to state the characterization of algebraic elements. So remember the situation that this A is algebra and x as a element there which is algebraic then we have this of algebra generated by x that is $K[x]$ which was isomorphic as a K algebra this is under the ϵ_x this is $K[X]/\langle \mu_x \rangle$ ideal generated by μ_x .

So x is algebraic then this, this is isomorphism in the, so that means the degree of this is μ_x so first thing to note here is if A may not be a field so first thing to note here is first thing to note is, if suppose A is an integral domain then this is a subring of which is sub-algebra of this so in particular subring so then, subring of an integral domain in real domain so this $K[X]$ is also an integral domain that means this residue class algebra mod μ_x is also integral domain because these are isomorphic algebras.

So and so $K[X]$ mod ideal generated by μ_x is also integral domain, but that means this ideal is a prime ideal.

(Refer Slide Time: 8:59)

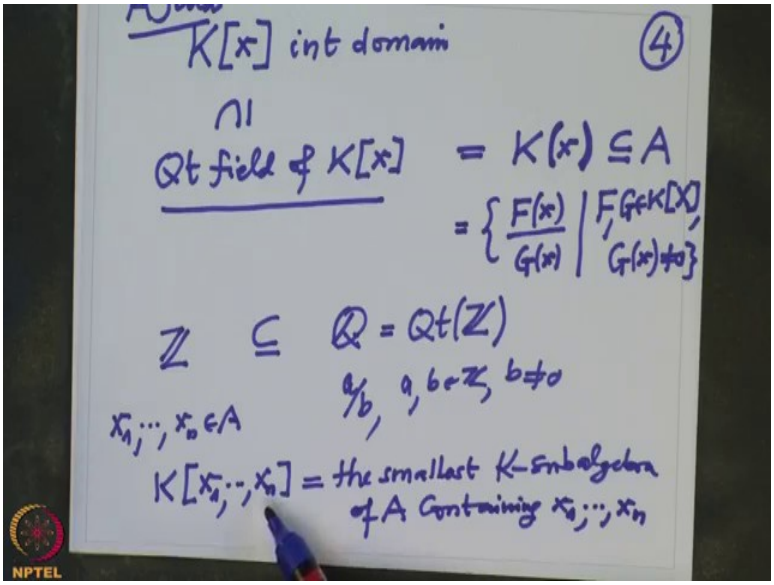


So that is the ideal, ideal μ_x is a prime ideal so that is then μ_x is a prime polynomial in the polynomial ring over K, let me remind you prime polynomial means a monic polynomial which is not a unit and it is it cannot split into two proper factors that means the only divisors are unit times that itself these are the prime polynomials. So for example, in $\mathbb{R}[X]$ we have seen what are the prime polynomials, if K were $\mathbb{R}$ the prime polynomials examples are monic am writing monic.

So one is $X-c$ this are linear ones and the other one is X^2+bX+c with the discriminant that is b^2-4c negative this are precisely the prime polynomials over $\mathbb{R}[X]$, over $\mathbb{Q}$ there are many-many infact given any degree we have a prime polynomial and many. So given $n \in \mathbb{N}$ X^n-P or X^n-pq all these are prime polynomials over $\mathbb{Q}$. So $\mathbb{Q}$ the theory will come more difficult over $\mathbb{R}$ it will be simpler because and the elements have C over $\mathbb{R}$ which can satisfy either linear polynomial or quadratic polynomial with the discriminant negative.

Ok, so now it is a if it is an integral domain let us take this case for because ultimately we want to concentrate on algebraic which are fields in fact but if it is a field then definitely μ_x is prime polynomial and then this $K[X]$ is an integral domain definitely.

(Refer Slide Time: 11:20)



Let us consider this case, in that case I can talk about its quotient field, so quotient field of this integral domain is usually denoted by K round bracket x, that means what? And why do you denote it by this notation? This means their rational function in x but they should make sense so that means what their fractions $\frac{F(x)}{G(x)}$ divided by $G(x)$ but then this should make sense, so F and G are two polynomials in K and the G cannot vanish at x, in particular G is not zero.

So take those fractions and that will form obviously as field is over a field so as shown where actually here now that A is a field or not necessary a field but then this may not be contained in K, definitely this make sense but it may not be contained in K, in K when A is a field actually this is small a is a field of A which this real domain is contained in it. So I think I hope you have seen the construction general construction of an quotient field of an integral domain from an integral domain. So that is the similar way we have seen in the school already that how do you construct $\mathbb{Q}$ from $\mathbb{Z}$ this $\mathbb{Q}$ is a quotient field of $\mathbb{Z}$, this is $\mathbb{Q}$ t $\mathbb{Z}$, I will denote standard notation I will denote $\mathbb{Q}$ t means the quotient field name.

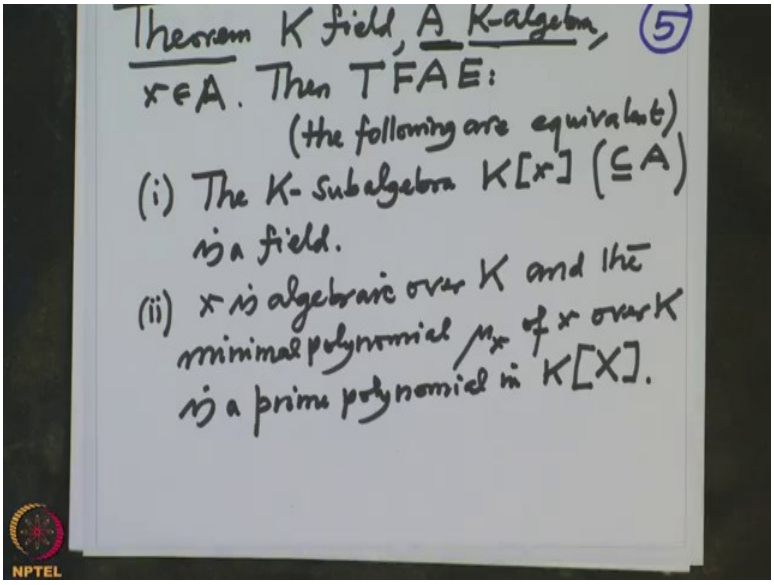
So you take the integers and take their fractions a by b where a, b are integers and b is non-zero such fractions is form a field and it is the smallest filed that z can contained, similarly for this so therefore this $K(x)$ is smallest field which contain this $K(x)$ and remember there is no

specially that this x is one element I could have done it for a bunch of elements namely I take the sub-algebra generated by that and if that sub-algebra is integral domain I will embed in a smallest quotient field and that, that is what the construction I am talking about.

If I have (small) if I have arbitrary elements x_1 to x_n and consider the sub-algebra generated by them, sub-algebra generated by them means the smallest sub-algebra of A which contain all this guys, this is the smallest K sub-algebra of A containing all this guys x_1 to x_n. So if this is an integral domain I have talked about the quotient field and then I will use the notation K round bracket x. So this is precisely what I keep saying in the earlier lecture that given a field I want to adjoin an element and make it a bigger field, this is for example bigger field.

I have adjoin the desk to the field, similarly here and then one element but many-many elements. So I will disgrace and this more elements more right now I concentrate only on one element and state our theorem which characterizes algebraic elements, so this is the theorem I am interested in doing.

(Refer Slide Time: 15:44)

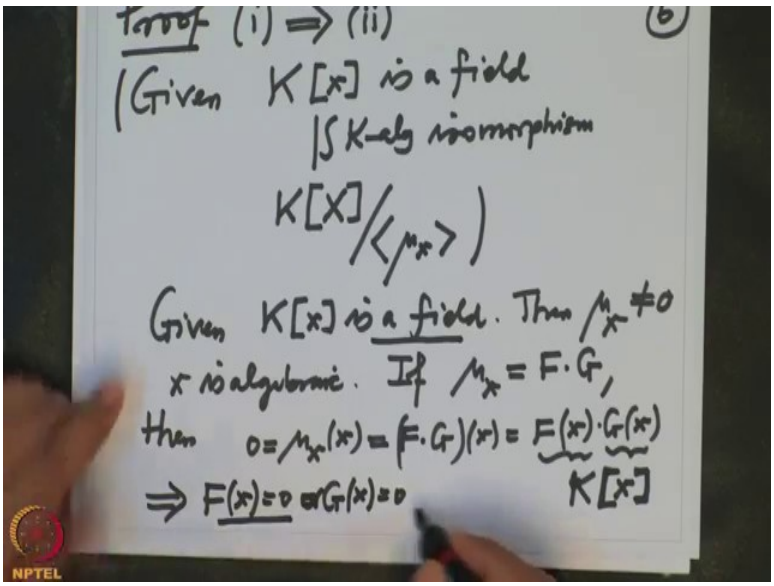


So, theorem, as usual K is a field A is a K algebra and x is an element in K, element in A and we want to know when this element is algebraic, so I am going to state equivalent condition, so one of them will be algebraic.

Ok, then and I will use this abbreviation all the time in the course The Following Are Equivalent, so this is the abbreviation for the following are equivalent, this is throughout the lecture, throughout my life I have used this because of my teacher ok so 1, the K, the sub-algebra the K sub-algebra $K[x]$, this is a sub-algebra of K generated by x is a filed. Remember what do you know? This is a sub-algebra and all elements are precisely the polynomials evaluated at that x and the condition 1 says it is already a field, 2, x is algebraic over K and the minimal polynomial μ_x of x over K is a prime polynomial in $K[X]$.

So you see, if you want to test somebody the algebraic you just have to check that the sub-algebra is a field, so it is an integral domain, here it may not be integral domain, it is a part of that, it is an integral domain and it is a field. Ok, so let us check that remember I am not assuring the field I am assuring you is only a K algebra, this is only a K algebra. So in this case sub-algebra is a field that is equivalent to saying x is algebraic so let us prove this.

(Refer Slide Time: 19:06)



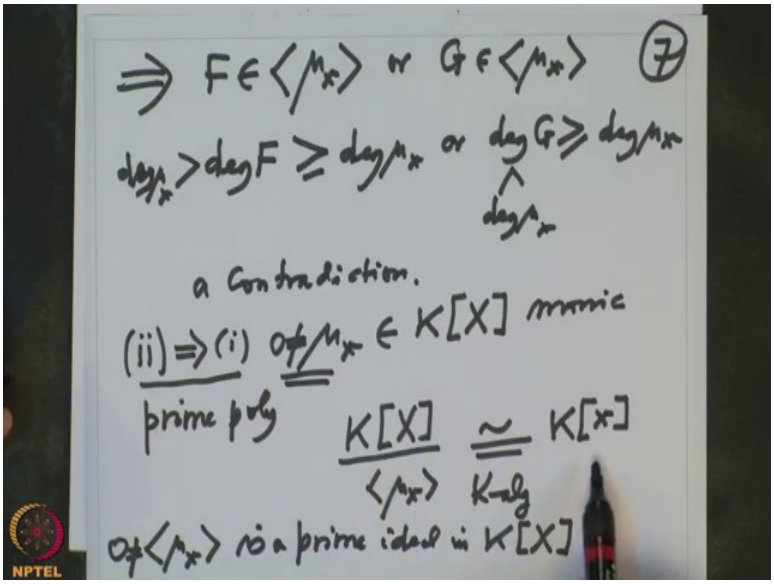
So proof, proof, so it gives the fieldness of this case of algebra not only gives information that x is algebraic but it also gives about the minimal polynomial that it is a prime polynomial alright, so (i) implies (ii) so I have given that, that sub-algebra is given $K[x]$ which is a field remember this is isomorphic as a K algebra to K polynomial x modulo ideal generated by the μ_x polynomial of x, this we know, this is by definition, this is a K algebra isomorphism, alright, so

this we know ok so the first thing I want to know what is, this μ_x has to be we have given this sub-algebraic a field, then I want to prove that, so this is just for recalling, what do you want to prove?

We have given this, so given, K x is a field then from this isomorphism we conclude that Mu has to be non-zero then μ_x has to be non-zero because if μ_x is zero then this (isomorphism) but this K is not a filed, K polynomial x is never a filed, so μ_x is non-zero but that already means that x is algebraic because algebraic means it should satisfy a non-zero polynomial and this is the minimal polynomial, this is non-zero means and x satisfies that means the Kernel is non-zero therefore x is algebraic, also and now I want to prove that it is a prime polynomial but if it is, so if suppose μ_x splits into two factors F and G then, then what do you know?

Then μ_x evaluated at x is zero that is by definition of μ_x, so this will be also F times G evaluated at x but this because it is an algebraic morphism evaluation in algebraic morphism so this is $F(x)$ and $G(x)$ and where are these elements? These elements are in K small x, this is this but this is to be a field and this product is zero in a field therefore each one of them will be zero. So that will imply $F(x)$ is zero also $G(x)$ is zero now $F(x)$ is zero or $G(x)$ is zero but $F(x)$ is zero will mean that so that will mean that F.

(Refer Slide Time: 22:49)



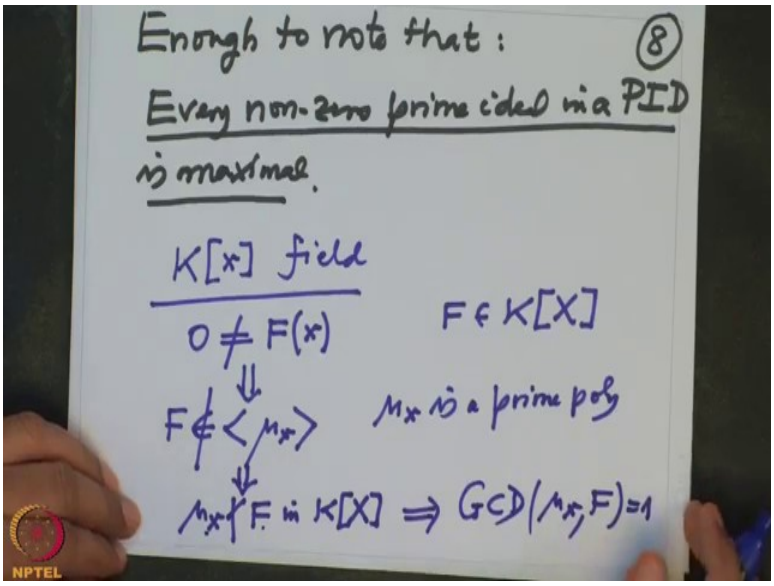
So that will mean that F belong to ideal generated by μ_x or G belong to the ideal generated by μ_x in particular the degree of F will be big or equal to degree of μ_x or degree of G will be big or equal to degree of μ_x but there is a integers factors they were proper factors of μ_x .

So this is to clear the degree μ_x this is also (())(23:25) degree μ_x or contradiction either this or this is a contradiction, a contradiction. So that proves that proves that if K small x is a field then x must be algebraic and the minimal polynomial should be prime polynomial. Now conversely that is two plus one they have given what did we give? What we have given? We have given that μ_x which is polynomial in $K[X]$ minimal polynomial, this is monic it is a prime polynomial and X is given to be algebraic, so that means this μ_x is non-zero given because (kernelly there are) generally has to be non-zero so it is prime polynomial and I want to prove that $K[x]$ is a field.

But that is also obvious because what do we know? We know that $K[X]/\langle \mu_x \rangle$ this is isomorphic, as K algebras to $K[X]$ and we want to (prove), this is a field, but I have given this is prime polynomial, so it is prime ideal.

So μ_x this is a prime ideal in $K[X]$ and non-zero prime ideal because μ_x is non-zero therefore now I want to use the fact that $K[X]$ is a principle ideal domain in that every non-zero prime ideal is maximal. Once i know that this μ_x will be a maximal ideal and residue class ring of a maximal ideal will be a field and therefore this will be a field.

(Refer Slide Time: 25:50)

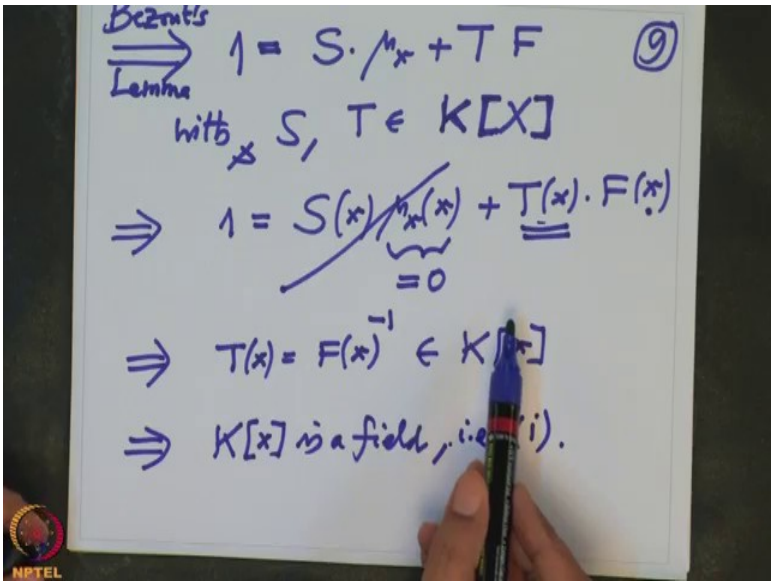


So enough to note that we have learned in earlier course, so enough to note that every non-zero prime ideal in a PID, PID stands for principle ideal domain is maximal. I will not prove this but I strongly recommend that you should check this on your own by recalling whatever you have learned in the first course in algebra mainly groups, rings, fields.

But this I can digress a little bit simpler way but you will have to use same technique to prove that every non-zero prime ideal in a PID is maximal. So what do you want to prove? I want to prove that this is a field so I will integrate for you that this is a field without using this, this is a field you want to check that alright. So that means they want given any element here non-zero, zero not equal to any element will look like $F(x)$ where F is a polynomial in coefficients in K.

I want to produce a inverse for this F, this means what? This means this F cannot belong to ideal generated by μ_x because μ_x this ideal precisely all those polynomials is vanish on x, so this is not there, that means and we know we have also given that this μ_x is a prime polynomial, μ_x is a prime polynomial. So that means μ_x cannot so this means μ_x does not divide $F \in K[X]$, this is a prime polynomial and this does not divide this so their GCD should be 1. So this means GCD of μ_x and F is 1, but you remember like integers GCD of two polynomials over a field is 1 then by linear combination of the two.

(Refer Slide Time: 28:24)



So that will imply I can write 1 as (what do have) $S\mu_x + TF$ with S and T two polynomials with coefficients in K this is known as the Bezout's lemma, this is what is true for integers and the same proof, same proof for polynomial as do it for integers because we know this polynomial ring has a factorization and the division algorithm that use the same thing. Now once you have this, now evaluate this, this is a polynomial of entity evaluate this at small x.

So that will imply 1, 1 you have evaluated as x is 1 only, S evaluated at x, μ_x evaluated at x plus T evaluated at x times F evaluated at x but μ_x is 0,because μ_x is minimal polynomial of x, so this term goes so 1 equal to T x times F x, so this T x is inverse of F x. So assuming the $F(x)$ is non-zero I have proved that it again inverse and this inverse belongs to K small x that means I have proved that this $K[x]$ is a field that is what the condition we wanted to prove which is 1, that is 1 satisfied.

So this is in some sense less technical but and also it gives you actually this method actually gives you how to produce inverse of F but soon or later we have to go and use higher high power machinery which will have vocabulary form what is called commutative algebra. Commutative algebra means prime ideal, maximal ideals and so on. So time to time I can give simpler proves and also use some new definitions to give little bit proves which involve more concepts that way one can learn more concepts easily through this examples.

So I will stop here and will continue about algebraic extension next time, next time I am going to attach a group to an algebraic extension and what will be called a Galois group and we will study the algebraic extension using this group and that interplay I will become I will make it more and more intemater so I stop here still next time, thank you.