

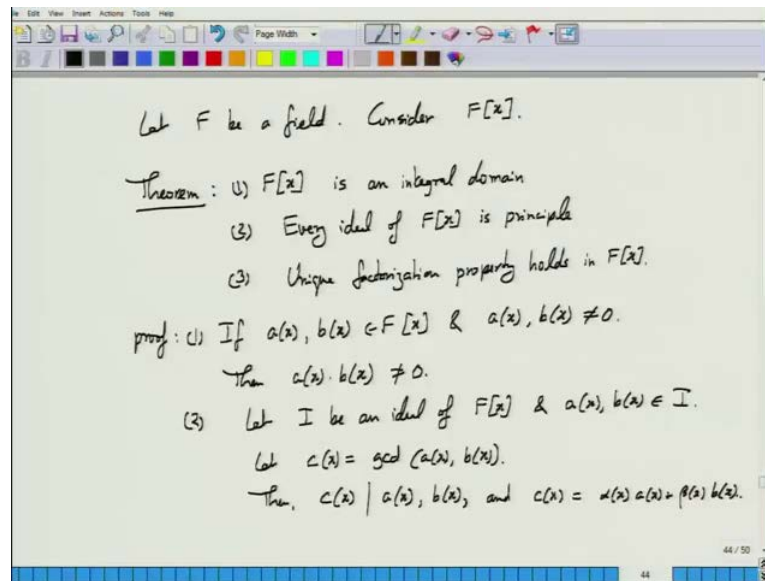
**Modern Algebra**  
**Prof. Manindra Agrawal**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kanpur**

**Lecture – 16**  
**Properties of Fields**

Now, let us continue our discussion about fields. Last time we proved this so called fundamental theorem of algebra. In fact, there is another fundamental theorem of algebra, which basically depends on who calls which one the fundamental theorem, which I will discuss little later in this, in the lecture. But like we saw last time, that every field has this nice property that integrity polynomial will have (Refer Time: 00:46).

Now, the one immediate question is of the, given a degree  $D$  polynomial over a field  $F$ , it will have at most  $D$  roots. The question next, the next one would be exactly how many of those  $D$  roots are actually in the field. It is possible, that there are 0 roots in the field. For example, in the, you know, look at polynomial  $x^2 + 1$  over the reals. It can have at most two roots, but actually it has, inside the real it has no roots. So, the numbers of roots will be lying between 0 and  $D$  and that is a very important part of investigations about polynomials over field and that also gives us a way to create more fields or extended field. So, let us look at that.

(Refer Slide Time: 02:03)



So, let us say, you start with a field and we consider  $F$  bracket  $x$ . This is the ring of univariate polynomials over field  $F$ . This ring has some nice properties. It is, for example,  $F[x]$  is an integral domain every ideal of  $F[x]$  is principle. Moreover, the unique factorization property holds in  $F[x]$ , but that here I am not saying, that  $F[x]$  is just a (Refer Time: 03:59) domain where the unique factorization or ideal holds, but element wise also, just like over  $\mathbb{Z}$ , element-wise unique factorization property holds similarly here not only over ideals. So, in that sense,  $F[x]$  is very similar to the ring of integers. See, that every ideal is principle unique factorization property holds is an integral domain, which are all very nice properties of integers.

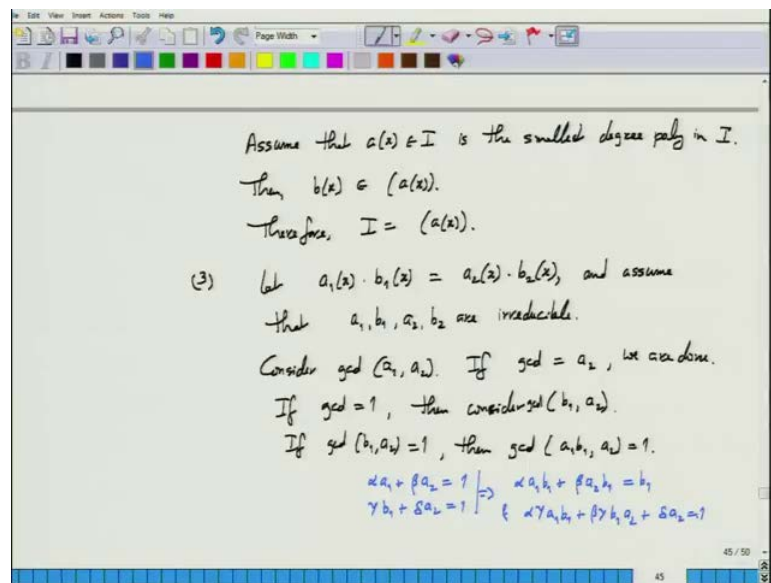
The first one is quite clear, that is,  $(a, b)$  in  $F[x]$  and they are non-zero. Then,  $a \cdot b$ , this polynomial will also not be 0. The reason is very simple. You take the highest degree term of  $a$ , highest degree term of  $b$ , their product will give the highest degree term of  $a$  times  $b$  and that coefficient will be non-zero. So, this is simply borrowing the fact, that  $F$  is an integral domain and therefore,  $F[x]$  will also be an integral domain, right. So, that takes care of the 1st property.

The 2nd one, every ideal in  $F$  is principle. So, take an ideal of  $F[x]$  and take two elements of this ideal. Oh, not  $F[x]$ , it is an, take two elements of the ideal. Now, we

have this operation available in  $F[x]$  over polynomials, that is, which was taking GCD of the polynomials. Just like we can take GCD of the numbers, we can take GCD of the polynomials and that, let that be  $C$  and then  $C$  divides  $a$  and  $b$  both, right. Or in other words, in addition we can write  $C$  as some, let us say,  $\alpha x + \beta$  right. So, this implies that  $C$  is also in the ideal  $I$ .

This equation is, essentially, just GCD algorithm that you give you this. So,  $C$  is in the ideal and both  $a$  and  $b$  are multiples of  $C$ , right. So, we can say, that  $a$  and  $b$  are in the ideal generated by  $C$ . So, with these two properties we will, we are done because now you start within the ideal  $I$ , the smallest degree polynomial that is present in the ideal  $I$ .

(Refer Slide Time: 09:06)



Now, take any other polynomial of the ideal  $I$ . So, let us say, assume, that let us say,  $a(x)$  in  $I$  is the smallest degree. Then, what can we say about  $C$ ?  $b$  is any other polynomial in the ideal  $I$ ,  $C$  must have the same degree as  $a$  and  $C$  divides  $a$ . That means,  $C$  is just a constant multiple of  $a$ , right, which means, that  $b$  is in the ideal generated by  $b$  is in the ideal generated by  $C$  and  $C$  is just a constant multiple of  $a$ . So, principle ideal of  $C$  is same as principle ideal of  $a$ . So,  $b$  is in the principle ideal of  $a$  and  $b$  was any arbitrary polynomial in the ideal  $I$ . So, this shows,  $I$  is simply the principle ideal generated by  $a$ .

And the third one, the unit factorization, well, let us assume, that  $a_1 \times b_1$  equals  $a_2 \times b_2$ . So, the real two factorization of one polynomial and we want to show, that these are, before that I need to define the notion of irreducible polynomial, that is okay, but that is already defined. Remember, I had defined the notion of irreducible element of a ring, which generalizes the notion of a prime number in integers. Irreducible element was an element such that whenever you write it as a product of two elements, one of those two elements is a unit.

So, suppose we can write a polynomial as a product of two irreducible elements,  $a_1, b_1, a_2, b_2$ .  $(a_1, b_1)$  is one set of irreducible elements,  $(a_2, b_2)$  is another set of irreducible elements. So, now I want to show, that this is the same, that is,  $a_2$  is equal to either  $a_1$  or  $b_1$  and similarly,  $b_2$  either equal to  $a_1$  or  $b_1$ .

Consider GCD of  $a_1, a_2$ . What is this going to be? This is either, both  $a_1, a_2$  are irreducible; either GCD would, whatever the GCD polynomial is, that divides both  $a_1$  and  $a_2$ . So, the, because they are irreducible, that GCD is either equal to  $a_2$  or 1. So, if GCD is equal to  $a_2$ , that means,  $a_1$  is equal to  $a_2$  except a constant multiplier. So, that is fine. Then, of course, we can argue the same way about  $b_1, b_2$  and we have done. On the other hand, if GCD equals  $a_2$ , we are done. If GCD equals 1, then, then consider GCD of  $b_1, a_2$ . This is the same thing. Again, this also will either be  $a_2$  or 1.

Student:  $a_2$  will divide  $b_1$ .

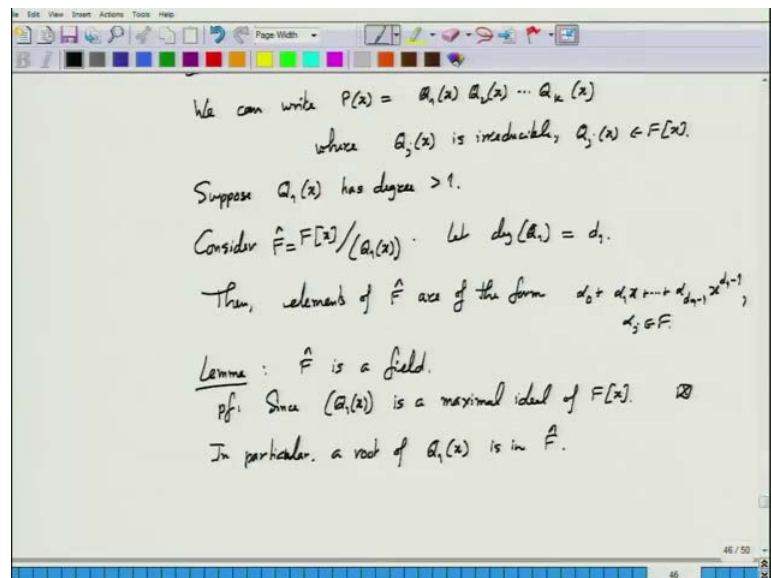
Yeah, see it is  $a_2$ . If it is  $a_2$ , then  $a_2$  and  $b_1$ , since both are irreducible are just constant multiples of each other, that is again there, we have, will be done, right, otherwise if this GCD is also 1, then that is a bad case for us. Then, what happens? We will show that it is not possible. How do we show that it is not possible? GCD, that is, GCD of  $a_1, a_2$  is 1 and GCD of  $b_1, a_2$  is 1. Let us look at what is GCD of  $a_1, b_1$  with  $a_2$  and I claim, that GCD of  $a_1, b_1$  with  $a_2$  is 1. Why? Well, it is just a bit of calculation, GCD of  $a_1, a_2, 1$  means what?

Student: (Refer Time: 16:38)

Alpha a 1 plus beta a 2 is 1, GCD of b 1, a 2 is 1 means what? Gamma b 1 plus delta a 2 is one. So, just combine these two, just multiply this with b 1. So, we get alpha a 1 b 1 plus beta a 2 b 1 is b 1 and multiply this with gamma alpha gamma a 1 b 1 plus beta gamma b 1 a 2 plus delta a 2 is 1. This is b 1 and b 1 you substitute in this, you get this equation and this gives me alpha gamma a 1 b 1 plus beta gamma b 1 plus delta a 2 is 1. So, this show, that GCD of a 1, b 1 and a 2 is 1. And that is not possible because clearly, a 2 divides a 1 b 1 by the assumption and that is it, and proves the theorem.

So, this ring  $F[x]$  bears very much like the ring of integers.

(Refer Slide Time: 19:03)



Now, let us consider, now its general column  $P(x)$  be in  $F[x]$ . This is polynomial degree  $d$  and let us goes back to that the fundamental theorem of algebra where we are looking at the roots of this polynomial  $P$  in the field  $F$ . So, unique factorization holds, I can write  $P(x)$ , let us say  $Q_1(x) Q_2(x) \dots Q_k(x)$ , where  $Q_j(x)$  is irreducible and this can be written uniquely. Now, if one can be say, that  $P$  has the root in  $F$  in terms of  $Q_1$  to  $Q_k$ .

Student: (Refer Time: 20:45)

Q has.

Student: (Refer Time: 20:53).

Q I is in  $F[x]$ , each one of them is in  $F[x]$ .

Student: (Refer Time: 21:00)

See, the fact that I can write here the product of this irreducible polynomial, each one of  $Q_j$  is in  $F[x]$  and that that is not in  $F$ .

Student: (Refer Time: 21:23)  $P(x)$  will be (Refer Time: 21:25).

Root of  $P$  will be root of one of them, yes, clear, right. If  $P$  is 0, then one of them will be 0 that is one conclusion we can derive. But suppose,  $\alpha$  is a root of  $P$  and  $\alpha$  is in  $F$ , can we say something about the nature of this, at least one of these  $Q_j$ 's? See, just go back to this proof. If  $\alpha$  was a root of  $P$ , then  $P$  can be written as  $(x - \alpha)Q(x)$  and which is  $x - \alpha$  times  $Q$  at  $x$ .

Student: Linear (Refer Time: 22:12).

Linear factor, so if  $\alpha$  is a root of  $p$  and  $\alpha$  is in  $F$ , then one of these  $Q_j$ 's will be of degree 1 and  $\alpha$  that will be actually of the form  $x - \alpha$  where  $\alpha$  is a root.

Student: Linear (Refer Time: 22:36).

Any linear polynomial is irreducible, of course.

Student: (Refer Time: 22:47).

Up to multiplication by unit; that multiplication by units is fine. So, that tells us

whether by looking at this factorization of  $P$  we can see how many roots of  $P$  are in  $F$  that equals the number of linear factors. So, there is no guarantee, that all of them are linear factors. So, some of them may not be linear factors. So, let us say, suppose  $Q_1(x)$  has degree greater than 1. So, it is not a linear factor.

Now, consider this ring,  $F[x]$  quotiented with the principle ideal  $Q_1$ . What can we say about this quotient ring?

Student: (Refer Time: 24:32).

Sorry.

Student: (Refer Time: 24:38).

Elements of this, it depends on the degree of  $Q_1$ , right, if the degree.

Student: (Refer Time: 24:50).

Let degree of  $Q_1$  be  $d + 1$ , then elements of  $F$ , let us call this, okay I will, I will be giving away the name, by name the nature. Elements of  $\hat{F}$ , this form where each element is a polynomial of degree at most  $d + 1$  minus 1 with coefficients being in  $F$  because you are quotienting with  $Q_1$ , which is a polynomial degree  $d$  quotienting with  $Q_1$ . Take any element, if  $F[x]$ , you would, can divide this again, just the GCD trick will give you a polynomial.

After taking, dividing you will get a residue, which will be of degree less than  $d + 1$  and that is the element in this. Strictly speaking, it is, the element is this plus the ideal. The elements of this quotient ring have the form  $a + I$ . So, this is  $a$  and plus the ideal. In that plus ideal  $I$  am not writing this to simply this, but you must keep in mind, that the elements of this quotient ring are not polynomials, they are equivalence classes. What else can we say about  $\hat{F}$ ? We, can say, that  $\hat{F}$  is a field.

Student: (Refer Time: 27:48)  $Q[x]$  is (Refer Time: 27:51).

$Q[x]$  is irreducible, yes, that is, that is by factorization, yeah, it follows because this ideal generated by  $Q[x]$  is a maximum ideal. We have seen, it is a principle ideal of course, principle ideal, but it is also a maximal ideal because  $Q[x]$  is irreducible. So, if there is any other take, any polynomial that is not a multiple of  $Q[x]$  is GCD with  $Q[x]$  will be 1 because  $Q[x]$  is irreducible, which means, that this principle ideal generated by  $Q[x]$  is maximum. And so,  $F$  hat is a field.

Student: (Refer Time: 29:07).

We do not need degree greater than 1, but if, what if  $Q[x]$  at degree 1, what is  $F$  hat? Then,  $F$  hat is just isomorphic to  $F$  because then, elements for the, the form  $\alpha_0$  plus the ideal you want that is just  $F$ . Whereas, if  $Q[x]$  has degree greater than 1, then we get a field  $F$  hat, which is not equal to  $F$ , it certainly contains  $F$ , but it contains elements more than  $F$ . Why are we sure that it contains element more than  $F$ ? Simply because all such elements are in the  $F$  hat of this, which are polynomials of degree less than 1 and these polynomials, these elements are not two such polynomials are not same in  $F$  hat. In particular, a root of  $Q[x]$  is in  $F$  hat. Do you see that?

Student: (Refer Time: 31:23)

What (Refer Time: 31:32) did not get that.

Student: (Refer Time: 31:33)

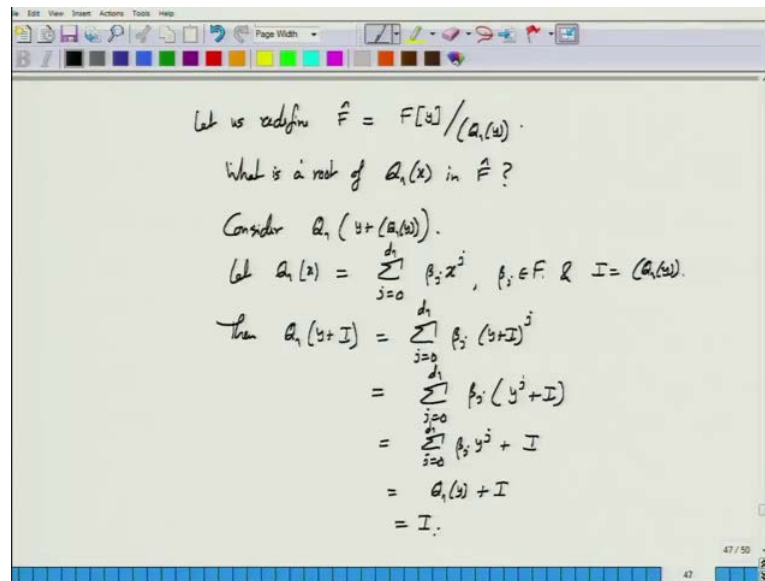
Classes corresponding to 0 that is, not root of  $Q[x]$ .

Student: (Refer Time: 31:38)

The  $Q[x]$  will map to 0, so that is fine, but in  $F$  hat I am claiming. So, what I should have done instead is, let us. That is an important point.



(Refer Slide Time: 32:08)



Let us redefine  $\hat{F} = F[x]/(Q_1(x))$ .

What is a root of  $Q_1(x)$  in  $\hat{F}$ ?

Consider  $Q_1(y + (Q_1(x)))$ .

Let  $Q_1(x) = \sum_{j=0}^{d_1} \beta_j x^j$ ,  $\beta_j \in F$ , &  $I = (Q_1(x))$ .

Then  $Q_1(y+I) = \sum_{j=0}^{d_1} \beta_j (y+I)^j$

$$= \sum_{j=0}^{d_1} \beta_j (y^j + I)$$
$$= \sum_{j=0}^{d_1} \beta_j y^j + I$$
$$= Q_1(y) + I$$
$$= I.$$

Let me, instead of doing it with  $x$ , let us redefine  $\hat{F}$  as  $F$  of  $y$  quotiented with  $Q_1$  of  $y$ . It is the same field, only thing that has happened is, instead of variable  $x$  I am using variable  $y$ . So, in the same field, in the sense, this  $\hat{F}$  is this field isomorphic to the field that earlier defined, fine.

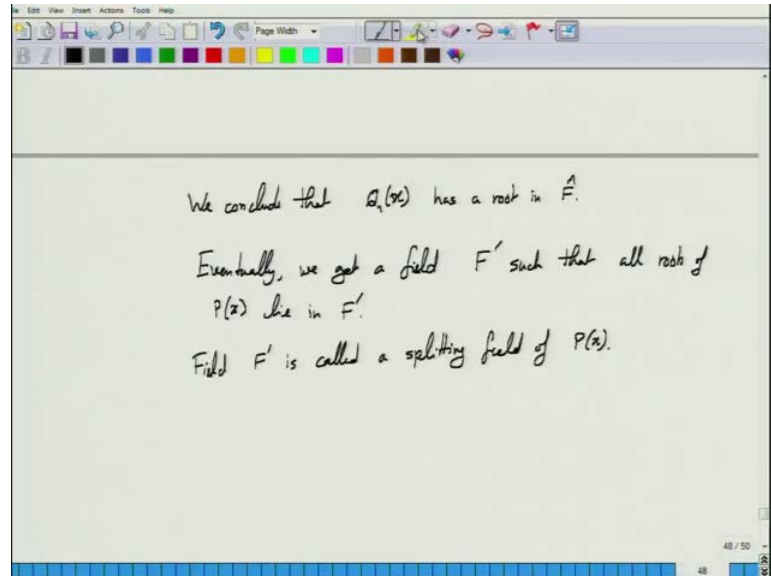
Now, I ask, what is a root of  $Q_1(x)$  in  $\hat{F}$ ? Consider  $Q_1(y + (Q_1(x)))$ . This is an element of  $\hat{F}$ . Now, I am writing it properly with the clear understanding, that this is an equivalence class. This equivalence class is an element of  $\hat{F}$ . So, if you replace  $x$  by this element of  $\hat{F}$  in  $Q_1$ , what do you get?

This would be  $Q_1(y + (Q_1(x)))$ ;  $Q_1(y)$ . You do not see that, let us do it more slowly; let me erase this. Let  $q_1(x)$  be this polynomial and do the substitution. Let us write  $I$  for this ideal. Is this fine? The moment I do this substitution,  $Q_1(y + I)$  is now becomes an element in the field  $\hat{F}$  because  $y + I$  is an element in  $\hat{F}$  and I am just doing some addition, multiplication using that element.

So, this is element in field  $\hat{F}$ , which element is this, this, carry out this arithmetic, this is field, you can do the arithmetic and we know exactly how do you do arithmetic on the quotient rings. This is same as; multiplication would mean,  $y + I$  raised to the  $j$

is same as  $y$  to the  $j$  plus  $i$ , correct. And this sum would be just the sum of this part plus  $I$ . This is  $Q^{-1}$  of  $y$  plus  $I$  and this is  $I$  because  $Q^{-1}$  of  $y$  is contained in  $I$ . So, therefore, what we got was, that  $Q^{-1}$  was this element  $y$  plus  $I$  is  $I$  in  $\hat{F}$ . So,  $y$  plus  $I$  is a root of polynomial  $Q^{-1}$  of  $x$  in the field of  $\hat{F}$ .

(Refer Slide Time: 38:47)



So, therefore we conclude, that  $Q^{-1}$  has a root in  $\hat{F}$ , which means,  $Q^{-1}$  is no longer irreducible in  $\hat{F}$ . So,  $Q^{-1}$  further factors in  $\hat{F}$ . So, I can write  $Q^{-1}$  as its irreducible factorization in  $\hat{F}$ . At least one of those factors is linear, if there may be still some higher degree factors. So, we can repeat this whole exercise with the higher degree factors. So, this iterative process will eventually give me a field, let us call it  $F'$ . Now, I do not want to call it  $F'$ ,  $F'$  prime, such that all roots of  $P$  of  $x$  lie in  $F'$  prime. There is a name for this particular field, is called as splitting field of the polynomial  $P$ .

All these fields, that we get starting from  $\hat{F}$  and continuing all way up to  $F'$  prime, these fields are called algebraic extensions of the field  $F$ . We started with  $F$ , we took a polynomial, which does not factor completely in  $F$  and used that polynomial to create a larger field and successively larger and larger fields till that point that that polynomial factors completely. So, all the field that we get in this sequence will, are algebraic

extensions. Yes.

Student: (Refer Time: 42:28) polynomial  $x$  (Refer Time: 42:30) minus  $x$  square plus 1 (Refer Time: 42:33).

Yes.

Student: (Refer Time: 42:34).

Yes, that is right, that is right.

Student: So, those which were already linear in  $F$  (Refer Time: 42:48).

They will stay, those root stay. See, any extension contains the smaller field, contains again in those, in the isomorphic sense, right, because now an element  $\alpha$  of  $F$  in  $\hat{F}$  becomes  $\alpha + I$ , that is, the corresponding element in  $\hat{F}$ , right.  $\hat{F}$  is quotient field, so the every element is in equivalence class. So, it is corresponding to  $\alpha$  in  $F$ . The element in  $\hat{F}$  is  $\alpha + I$ . So, this is what an algebraic extension is.

One of you asked in the last class, how, what is algebraic, how do elements of algebraic extension look like? This is exactly what they look like. They are polynomials of a certain degree in the base field, the starting field. The key thing is, that we must start with a field, look at the ring polynomials, quotient it with the irreducible polynomial of degree more than 1, we get extension field which contains the original field. Its elements are polynomials in the base field. Again, when I say polynomial, this is strictly speaking not true because they are equivalence classes of polynomials. What I am just going to continue saying, they are polynomials because it is kind of easier to describe that way.

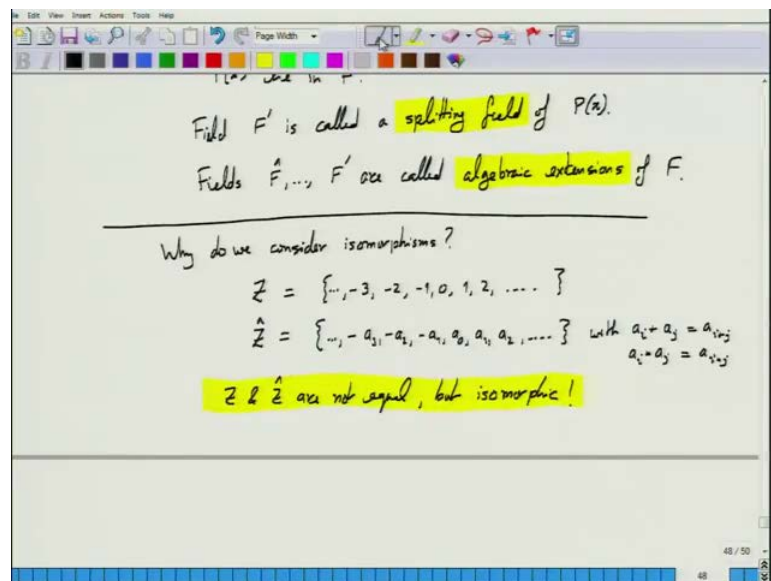
Student: (Refer Time: 44:45)

Two fields are isomorphic we take them to be equal, not equal, you are right, they are not identical. But if two fields are isomorphic, then you can treat them as identical.

Student: Can a ring be isomorphic (Refer Time: 45:13).

A ring, so if two rings are isomorphic and one of them is a field, other has to be a field, it has to be that. See, the isomorphism means, both additions, multiplication are preserved. So, if  $a$  times  $b$  is 1 in 1, then 5 of times 5  $b$  would be 1 in the other, so that means, the inverse will also exist in the other. So, that is, isomorphism essentially, you know, captures the same field. In fact, it has to use a notion of isomorphism.

(Refer Slide Time: 45:57)



Just to take a side issue, why do we consider isomorphism? Well, let me define ring of integers as this. Now, integers are, this is a usual way of defining ring of integers, let me define the following. This is a collection of different set of elements, the names, the symbols I am using are different, but the operations in both these rings are go in the essentially the same way,  $a + b$  is  $a$  plus  $b$   $a \cdot b$  is  $a$  times  $b$ .

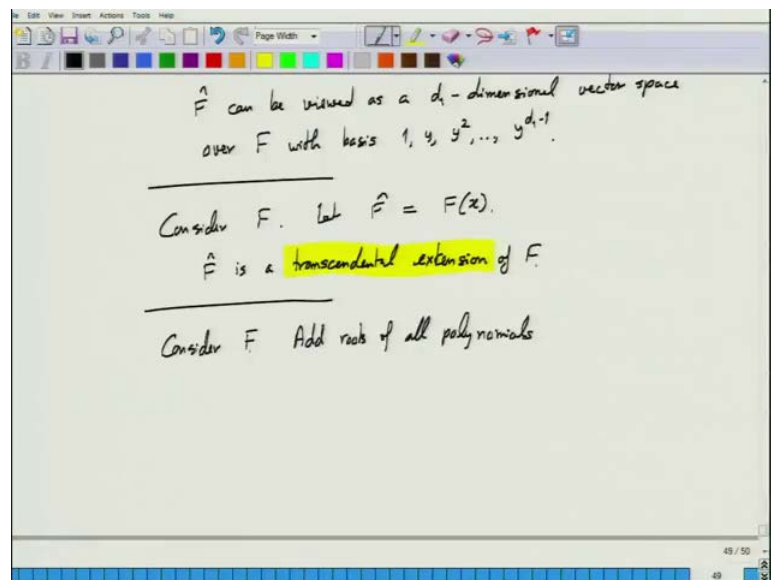
Would you say that this is also ring of integers? It is just that I am choosing, it is a choosing symbol 0, 1 to represent numbers. I am choosing different symbols to

represent the ring, but they are both, they represent essentially the same entity, and the only way I can establish the equitance between them is true isomorphism. They are not equal, but they are isomorphic and that is why, when two objects, algebraic objects are isomorphic, we treat them as identical, alright. Yes.

Student: (Refer Time: 49:05)

How do we see vector space? Now, you tell me.

(Refer Slide Time: 49:20)



Go back to the example, consider  $\hat{F}$ , what were the elements of  $\hat{F}$ ?  $\hat{F}$  had as elements polynomials in  $y$  of degree less than  $d_1$  plus  $I$ , of course. This  $I$  we will ignore continually, that is basically the zero elements. Now if you just look at polynomials in variable  $y$  of degree less than  $d_1$ , this forms a vector space over  $F$ . I can view  $\hat{F}$  as a  $d_1$  dimensional vector space over the field  $F$  with basis  $1, y, y^2, \dots, y^{d_1-1}$ . Any element of  $\hat{F}$  can be written as a linear combination of these  $d_1$  elements and these are linearly independent also. So, that is, falls out of the way we have created extensions.

Student: Scalar multiplication (Refer Time: 51:30).

Scalar multiplication is through  $F$ . Any element of  $F$  is treated as scalar here. So, now, the next question is, we now understand the algebraic extension of a field, are there other types of extensions of a field? So, you start with, extension is basically you start with a field and create a bigger field. So, algebraic extension we have seen, how to do that? There are, there is one more very important type of extension of a field, which is called transcendental extension.

So, again start with a field  $F$  and let  $F^{\text{hat}}$  be the field of all rational functions in the variable  $x$  over  $F$ . This field  $F^{\text{hat}}$  is a transcendental extension of  $F$ ; this is clearly not an algebraic extension. Firstly, it is an extension because  $F^{\text{hat}}$  contains  $F$ , but there is really no polynomial involved in this extension. Another way of seeing, that  $F^{\text{hat}}$  is not a finite dimensional vector space over  $F$  because it contains polynomials of arbitrary high degree as elements. So, non-algebraic extensions which include an infinite dimensional extension are called transcendental extension, but this is not of much interest for us. We will not really worry too much about this.

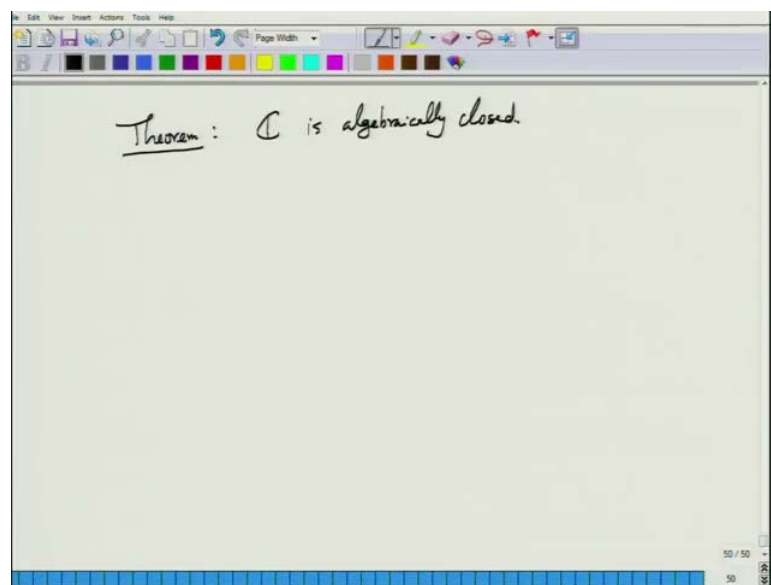
Let us get back to the algebraic extension. So, is it and ask the following, is it that we can do an algebraic extension from any field, that is, take any field, can we do an algebraic, find an algebraic extension of that field which is larger than this? The answer is no for the simple reason, take a field, consider  $F$ , let us say starting, take a polynomial and go to the splitting field of  $F$  with respect to that polynomial. Then, take another polynomial over  $F$  prime and go to the splitting field of that polynomial with respect to  $F$  prime and keep doing this process. So, essentially just keep of course, this is an effectively long process, but you will eventually have a field which contains roots of all polynomials in it, okay.

So, add roots of all polynomials. This is a little informal that notion, that I am giving you because I am not precisely defining it. So, let me, instead of that let us just go to the definition. So, we have a field  $F$  where every polynomial over  $F$  has a root in  $F$ , then such a field is called algebraically closed field because you cannot extend this anymore algebraically. You take any polynomial that has a root in  $F$ , take that root out, it gives you, get  $a$ , get another polynomial of lower degree that will also have root in it. So, every polynomial of degree  $d$  will have exactly  $d$  roots in this, such a field  $F$ , and so, it

is not possible to algebraically extend such a field.

And earlier, what I informally talked about, keep extending it, keep extending it forever gives a way to visualize that there exist an algebraically closed field, but that is kind of not a very concrete example. So, in the next class I will not, well, do not prove, that actually is none, let me just end up with a theorem.

(Refer Slide Time: 57:53)



The field of complex numbers is algebraically closed. This is also called fundamental theorem of algebra.

Student: (Refer Time: 58:18).

Sorry.

Student: (Refer Time: 58:23).

Yes, every polynomial of degree  $D$  has exactly  $D$  roots over complex numbers.