Introduction to Rings and Fields

Prof. Krishna Hanumanthu

Department of Mathematics

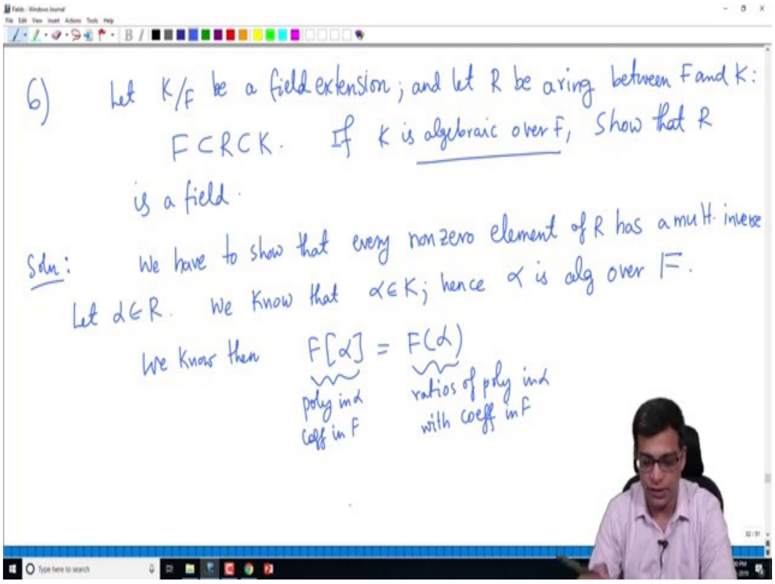
Chennai Mathematical Institute

Lecture - 44

Problems 11

Let us continue. Now, we started doing some problems on field theory in the previous video. So, we are going to continue and do some more problems and this will be the last video of the course, ok.

(Refer Slide Time: 00:28)



6) Let K/F be a field extension; and let R be a ring between F and K: $F \subset R \subset K$. If K is algebraic over F, Show that R is a field.

Sdn: We have to show that every non zero element of R has a mult. inverse

Let $\alpha \in R$. We Know that $\alpha \in K$; hence α is alg over F.

We Know then $\underbrace{F[\alpha]}_{\text{poly in } \alpha \text{ coff in } F} = \underbrace{F(\alpha)}_{\text{ratios of poly in } \alpha \text{ with coeff in } F}$

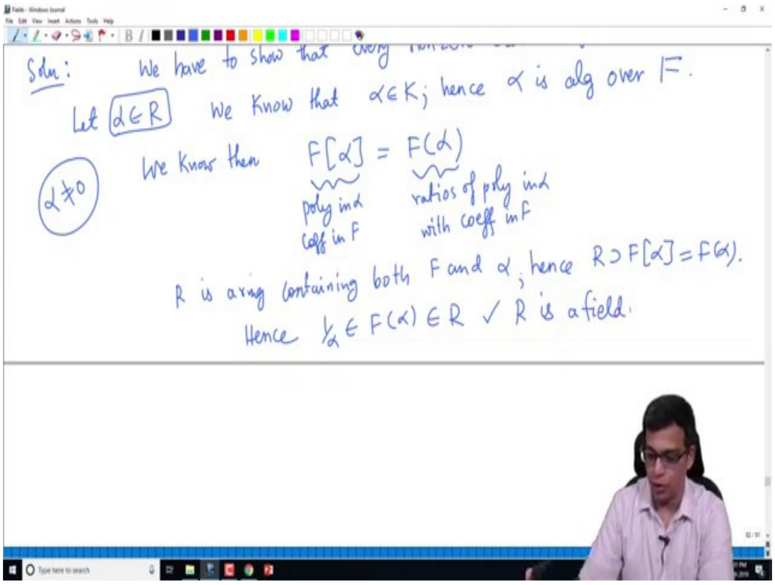
So, let us continue the Problems, this is the 6th problem. Let F and K be fields. So, actually let K be a field extension of F. So, let K over F be a field extension, and let R be a ring between F and K. So, I will explain what; that means, it is what we have is that F is contained in R, contained in K. So, F and K are field and R is between them. If K is algebraic over F, show that R is also a field, ok.

So, this exercise says that, if you have an algebraic extension any ring in between is automatically a field. So, this is a simple proof actually simple solution, but it is a very nice statement. It says that any ring in between two fields, when the bigger field is algebraic over the smaller field is automatically a field. What do you have to show? So, we have to show that every non-zero element of R has a multiplicative inverse, that is all, right, ok.

So, what do we do? So, let us take let alpha be an arbitrary element in R, we know that alpha is in K right, because R is a subring of K. And hence alpha is algebraic over R, sorry algebraic over F, because K is algebraic over F that is the hypothesis, so alpha is algebraic over F. So, these from the very beginning of the field theory part of this course we know then, that F alpha is actually equal to F round bracket alpha. This is the polynomials in alpha, these are ratios of polynomials in alpha with coefficients in F, these are polynomials with coefficients in F.

Remember F square bracket alpha always for us represents the polynomial ring, round bracket alpha represents the field; that means, it is ratios of polynomials because alpha is algebraic over F, this is the case.

(Refer Slide Time: 03:13)



Sdn: We have to show that every

Let $\boxed{\alpha \in R}$ We Know that $\alpha \in K$; hence α is alg over F.

$\boxed{\alpha \neq 0}$ We Know then $\underbrace{F[\alpha]}_{\text{poly in } \alpha \text{ coeff in } F} = \underbrace{F(\alpha)}_{\text{ratios of poly in } \alpha \text{ with coeff in } F}$

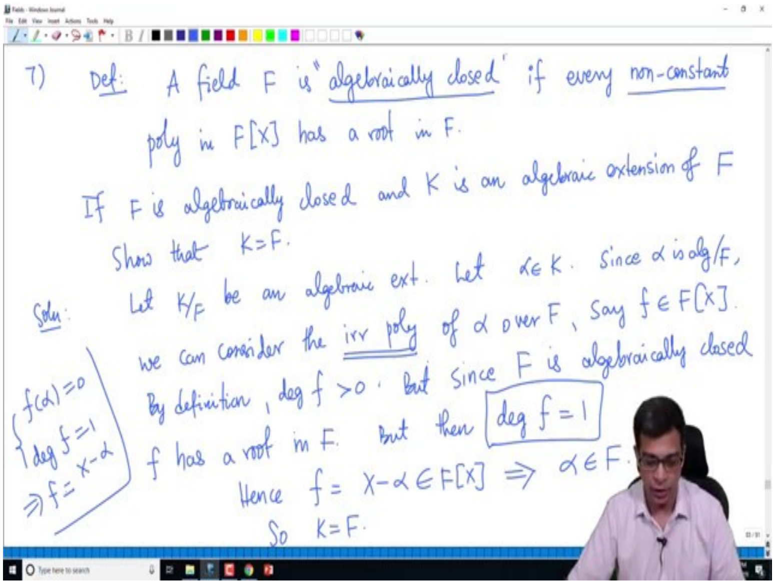
R is a ring containing both F and α; hence $R \supset F[\alpha] = F(\alpha)$.

Hence $1/\alpha \in F(\alpha) \in R$ ✓ R is a field.

But, then R is a ring containing both F and alpha, remember we took alpha in R and of course, F is contained in R that is hypothesis. So, it contains both F and alpha, hence R contains F square bracket alpha, because F square bracket alpha is the smallest ring containing F and alpha in K. It is the smallest ring. So, R contains them. So, R is going to contain F alpha also, but that as we just observed is same as F 1 by alpha.

Hence of course, here I should take alpha to be non-zero because if it is already in F, there is nothing to do so we might as well assume that alpha is not an F. And hence one by alpha which is in F alpha is in R, ok. So, R is a field there is nothing more to do here right. So, this is clear. So, if you have a ring squeezed in between an algebraic extension of fields, this is automatically a field.

(Refer Slide Time: 04:19)



7) Def: A field F is "algebraically closed" if every non-constant poly in F[X] has a root in F.

If F is algebraically closed and K is an algebraic extension of F Show that $K=F$.

Soln: Let K/F be an algebraic ext. Let $\alpha \in K$. Since α is alg/F, we can consider the irr poly of α over F, say $f \in F[X]$. By definition, $\deg f > 0$. But since F is algebraically closed f has a root in F. But then $\boxed{\deg f = 1}$

Hence $f = X - \alpha \in F[X] \Rightarrow \alpha \in F$.

So $K = F$.

$\left\{ \begin{array}{l} f(\alpha)=0 \\ \deg f = 1 \end{array} \right.$

$\Rightarrow f = X - \alpha$

So, next problem; so, I am going to nice definition I did not have time to discuss such fields in this course, but this is an important notion of fields, it is called an algebraically closed field. So, a field F is algebraically closed so, this is the terminology, a field F is algebraically closed, if every non-constant polynomial in F X has a root in F.

So, remember that the entire field theory course we are studying; the most important thing we are starting is given a field and a polynomial in it over it, we are we have learned how to construct a bigger field where the polynomial has a root, that we have learned. The procedure to do that in general we have learned, but algebraically closed fields are those fields, where that procedure is not needed, every polynomial has a root there. I need to insist on non-constant polynomial because certainly nonzero constants cannot have roots.

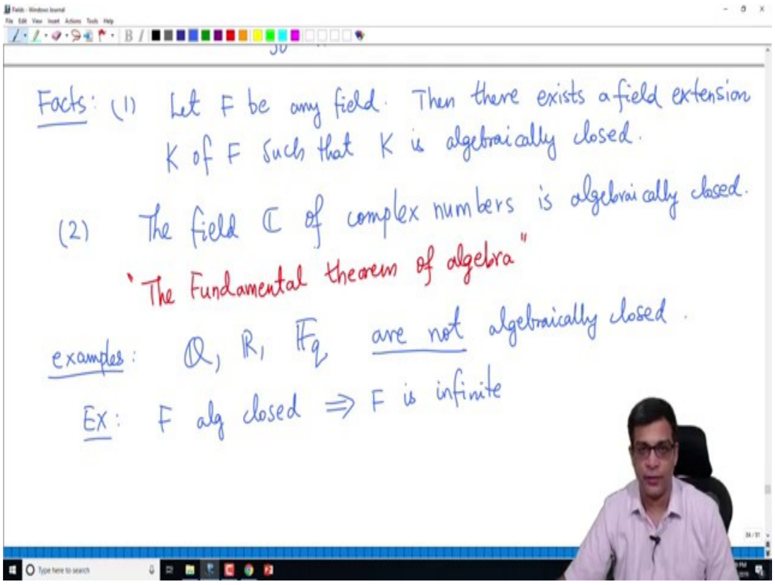
So, every non-constant polynomial has a root in F. There are such fields I will give you one example in a minute, but the exercise here is to show that, if F is algebraically closed and K is an algebraic extension of F show that K equal to F. So, the exercise is showing that, there cannot be a nontrivial algebraic extension of an already algebraically closed field. So, solution for this is again very simple. Let K over F be an algebraic extension. Let alpha be in K, we will actually show that alpha is also in F.

So, since alpha is algebraic over F, we can consider the irreducible polynomial of alpha over capital F, say f. So, let us take the irreducible polynomial of alpha over capital f. So, by definition remember degree of f is positive. Because it is an irreducible polynomial so; that means, it is a positive degree polynomial. And f is irreducible in capital F X. But, since capital F is algebraically closed, that is the hypothesis, small f has a root in capital F.

Remember, what is our definition of an algebraically closed field? It says that every non constant polynomial with coefficients in F has a root in F, small f is a non constant polynomial with coefficients in F, so it has a root in F, but then degree of f must be 1, right. This is the only possibility because if it is greater than 1, it because it is irreducible it cannot split, but it has a factor coming from the root. So, degree of F is 1 and hence f must be X minus alpha. Because f has alpha as a root right, f alpha is 0, degree of free is 1, these 2 together imply that f must be X minus alpha. There can’t be any extra factor there because then it will not be irreducible.

So that means, remember X minus alpha, f is in F X so, X minus alpha is in F x; that means, alpha is in F. So, K is equal to F ok. So, that is all. So, any algebraic extension of an algebraically closed field is automatically equal to the field that you started with. So, every non-trivial extension of an algebraically closed field has to be transcendental, we cannot contain any algebraic elements.

(Refer Slide Time: 08:57)



Facts: (1) Let F be any field. Then there exists a field extension K of F such that K is algebraically closed.

(2) The field $\mathbb{C}$ of complex numbers is algebraically closed.

"The Fundamental theorem of algebra"

examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_q$ are not algebraically closed.

Ex: F alg closed $\Rightarrow$ F is infinite

So, I will give you a couple of facts here which you may use in exercises and exams and homeworks and you will learn these in a different course. First fact is that, let F be any field, then there exists a field extension K of F such that, K is algebraically closed.

So, this fact says that every field sits inside an algebraically closed field ok. This is a construction that is not difficult, it requires some Zorn's Lemma argument we have used in showing that there exists a maximal ideal in every ring. But, it can be done, I do not have time to do this, but it is a fact that every field sits inside a big field which is algebraically closed, we can use this, if needed in exercises.

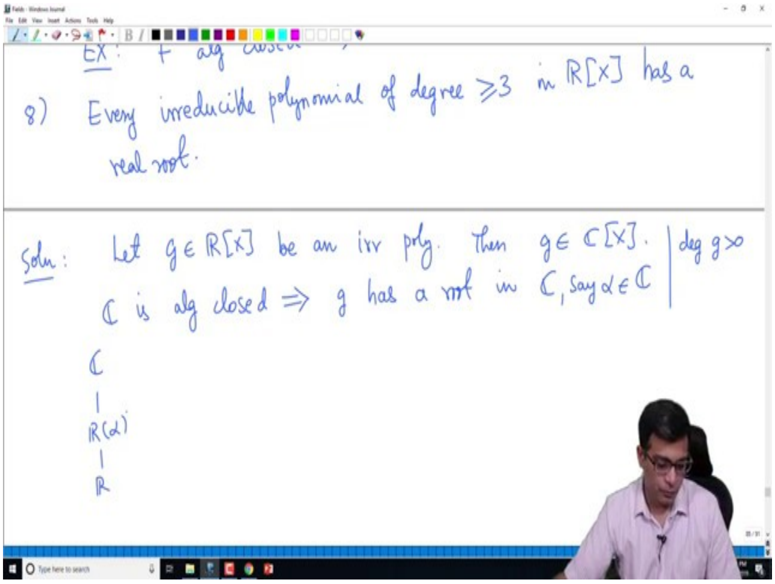
Second is a more concrete fact: the field of complex numbers, which we denote by C, is algebraically closed, ok. So, this is often called the fundamental theorem of algebra, this is a very important theorem as the name suggests it is called the fundamental theorem of algebra. It is also famous because it has lots of proofs using different fields of mathematics; topology, analysis, algebra, so there are lots of proofs of this and you may have seen some proofs in other courses, you will see some proofs of this.

So, the field C is algebraically closed; that means, the statement one, that I wrote here is automatically true for any subfield of C. Which is actually, some of the most important fields that we studied in this course. So, Q, R, Q adjoined root 2 all these fields, are contained in an algebraically closed field, but you can do better than C for many of them and that is called algebraic closure. There is sort of a minimal way of constructing an algebraically closed field containing a given field, but let me not get into that ok. These two facts we will use and as examples of non-algebraically close fields, we immediately see that Q, R, Z mod p Z more generally F Q are not algebraically closed, ok.

So, these are standard fields that we study, but they are not algebraically closed, I will leave the explanations for you Q for example, R in general is not algebraically closed because X squared plus 1 has no root. There are degree 2 polynomials which do not have roots in R, so that is not algebraically closed. F q is not algebraically closed, because it is a finite field. One can show that as an exercise I will not do this, but I will leave this for you, F algebraically closed which I will shorten it like this implies F is infinite.

The point is you can consider lots of irreducible polynomials, infinitely many and each of them has a root. So, that forces F to be infinite. So, in particular F q cannot be algebraically closed; however, each of these fields is contained in an algebraically closed field. Q and R it is trivial because C contains it, contains them. F q you have to work and use the fact one and that involves some construction and applications of Zorn's Lemma to conclude that F q is also contained in an algebraically closed field, ok. So, along these lines I want to do one exercise, which is number 8 and that is the following.

(Refer Slide Time: 12:49)



EX: F alg closed

8) Every irreducible polynomial of degree ≥ 3 in $\mathbb{R}[x]$ has a real root.

Soln: Let $g \in \mathbb{R}[x]$ be an irr poly. Then $g \in \mathbb{C}[x]$. | deg $g > 0$

$\mathbb{C}$ is alg closed $\Rightarrow$ g has a root in $\mathbb{C}$, say $\alpha \in \mathbb{C}$ |

$$\begin{array}{c}\mathbb{C}\\ | \\ \mathbb{R}(\alpha)\\ | \\ \mathbb{R}\end{array}$$

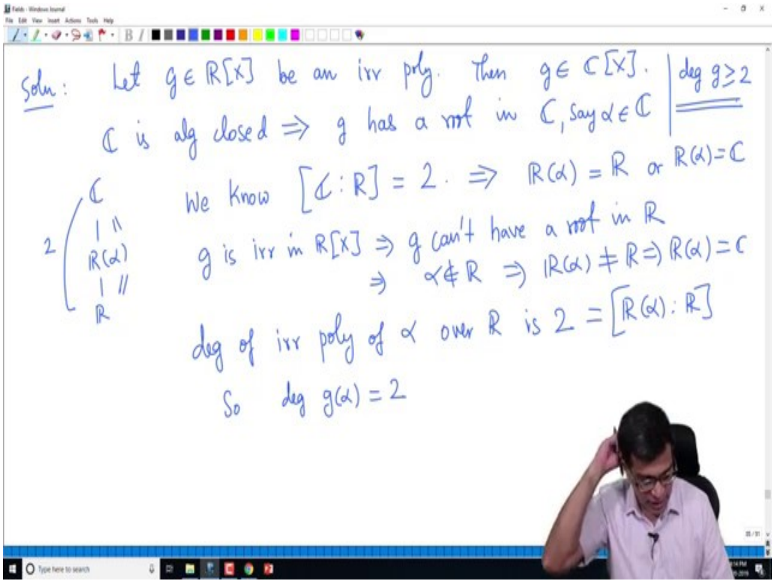
So, let show that every irreducible polynomial so, I just commented in the just now, that real number field is not algebraically closed, algebraically closed because there are degree two polynomials which have no roots. For example, X squared plus 1, has no root.

In this exercise will show that, any degree 3 or higher polynomial which is irreducible has a root, has a real root.

So, while there are irreducible degree 2 polynomials, there cannot be any irreducible degree 3 polynomials, irreducible degree 4 polynomials and so on. So, the solution is going to use the fact that I wrote, that C is algebraically closed, but then the proof is, solution is easy.

So, let g be an irreducible polynomial with real coefficients. Then of course, g is inside C X also right. Now, C is algebraically closed implies g has a root in C. Because it is an irreducible polynomial and hence degree of g is automatically positive and C is algebraically closed means, every root has every non constant polynomial has a root. So, say alpha, ok. So, degree g is positive. So, it has a root say alpha in C; now look at the field extension C, R alpha and R, ok.

(Refer Slide Time: 14:46)



Soln: Let $g \in \mathbb{R}[x]$ be an irr poly. Then $g \in \mathbb{C}[x]$. | deg $g \geq 2$

$\mathbb{C}$ is alg closed $\Rightarrow$ g has a root in $\mathbb{C}$, say $\alpha \in \mathbb{C}$

$$\begin{tikzcd} \mathbb{C} \arrow[d, dash, "\shortparallel"] \arrow[dd, bend right=60, dash, "2"'] \\ \mathbb{R}(\alpha) \arrow[d, dash, "/\!/"] \\ \mathbb{R} \end{tikzcd}$$

We know $[\mathbb{C} : \mathbb{R}] = 2.$ $\Rightarrow$ $\mathbb{R}(\alpha) = \mathbb{R}$ or $\mathbb{R}(\alpha) = \mathbb{C}$

g is irr in $\mathbb{R}[x] \Rightarrow$ g can't have a root in $\mathbb{R}$ $\Rightarrow \mathbb{R}(\alpha) \neq \mathbb{R} \Rightarrow \mathbb{R}(\alpha) = \mathbb{C}$

$\Rightarrow \alpha \notin \mathbb{R} \Rightarrow$

deg of irr poly of α over $\mathbb{R}$ is $2 = [\mathbb{R}(\alpha) : \mathbb{R}]$

So deg $g(\alpha) = 2$

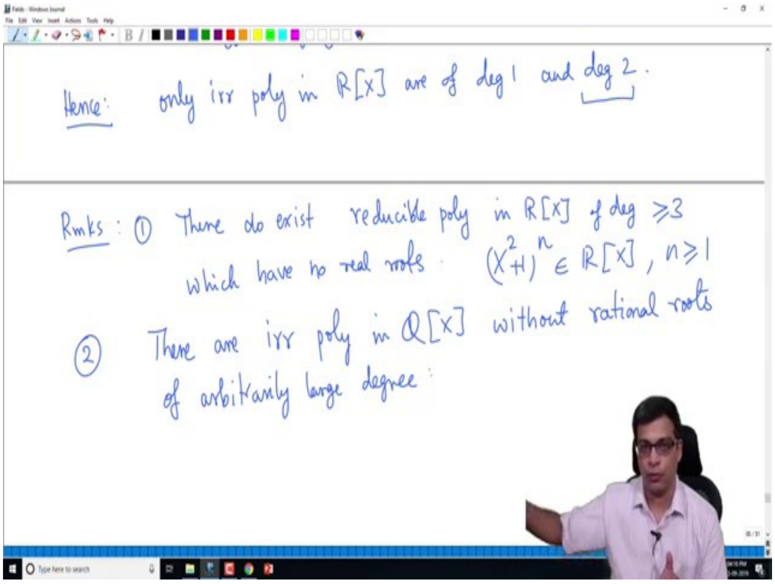
So, this means note that we know the degree extension of C right over R this is 2. This is one of the examples I gave when I defined degree of field extensions; I, 1 comma I is a basis of this. So, remember an exercise that I did in the last video of course, that exercise is not needed here, but it is a good chance for me to recall that exercise.

If you have an extension of prime degree there are no proper intermediate fields. So, R alpha is equal to R or R alpha is equal to C. This is either equal to this or equal to this, but g is irreducible in R x; that means, it cannot have a root; that means, alpha cannot be in R; that means, R alpha is not equal to R, but that means, R alpha is equal to C. But, then degree of the irreducible polynomial of alpha over R is 2, because this is the extension degree right, because this is C.

So, degree of the irreducible polynomial of alpha over R is 2, but what is the irreducible polynomial of alpha over R? It must be g right, because g is already irreducible. Alpha is a root of g; so degree of g. So, actually I should have said here that g assume is actually greater than equal to 2. Because if it is degree 1, there is nothing that we need to do, that case will correspond to R alpha equal to R; that means, alpha is already in R.

So, assume that degree g is at least 2. Then, we have concluded that it must be exactly equal to 2, hence only irreducible polynomials in R X, R of degree 1 and degree 2. These are the only possible degrees for irreducible polynomials.

(Refer Slide Time: 16:48)



Hence: only irr poly in $\mathbb{R}[X]$ are of deg 1 and $\underbrace{\text{deg } 2}$.

Rmks: ① There do exist reducible poly in $\mathbb{R}[X]$ of deg ≥ 3 which have no real roots. $(X^2+1)^n \in \mathbb{R}[X]$, $n \geq 1$

② There are irr poly in $\mathbb{Q}[X]$ without rational roots of arbitrarily large degree.

Remember, what is an algebraically closed field, there is every non-constant polynomial has a root; another way of saying this is degree of irreducible polynomial has to be 1. There cannot be a polynomial of degree 2 or 3 or higher which is irreducible. R is very close to that, R does not quite have the property of being algebraically closed, but it is very close.

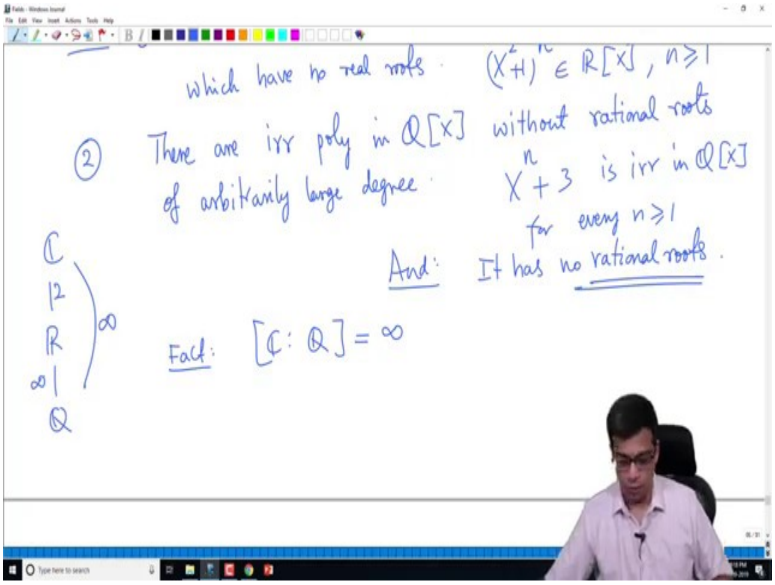
Because it has one additional degree, that is possible for irreducible polynomials, but not anything else. So, 3, 4 and so on is not there. And that is reflected in the fact that there is a degree 2 extension of R, which is algebraically closed ok. Just you go one step more from R you get algebraically closed. So, R is very close with the algebraic closure or being algebraically closed, but it is not quite true.

So, just couple of remarks I want to make coming from this exercise; there do exist non-irreducible or reducible polynomials in R X of degree greater than equal to 3 which have no roots. Right, because for example, you take X squared plus 1 power 2, this is a degree for polynomial, but it has no roots.

So, reducible polynomials can have can fail to have roots, but irreducible polynomials cannot exist of degree 3 or more. Whereas, any degree you can take, X Square plus 1 power n, where n is at 1, this has no roots. So, you get arbitrarily large degree polynomials, which are which do not have real roots, but remember these are not irreducible, they are reducible as soon as n is at least 2.

The other remark is there are irreducible polynomials in Q X without roots rational roots of arbitrarily large degree. What was nice about R was there cannot be irreducible polynomials without real roots of degree 3, 4, 4, 5 and higher, but that is not the case for Q X. Q is in other words very far from being algebraically closed.

(Refer Slide Time: 19:42)



which have no real roots. $(X^2+1)^n \in \mathbb{R}[X]$, $n \geq 1$

② There are irr poly in $\mathbb{Q}[X]$ without rational roots of arbitrarily large degree. $X^n + 3$ is irr in $\mathbb{Q}[X]$ for every $n \geq 1$

And: It has no rational roots.

$$\begin{tikzcd}
\mathbb{C} \arrow[d, dash, "2"'] \arrow[dd, dash, bend left, "\infty"] \\
\mathbb{R} \arrow[d, dash, "\infty"'] \\
\mathbb{Q}
\end{tikzcd}$$

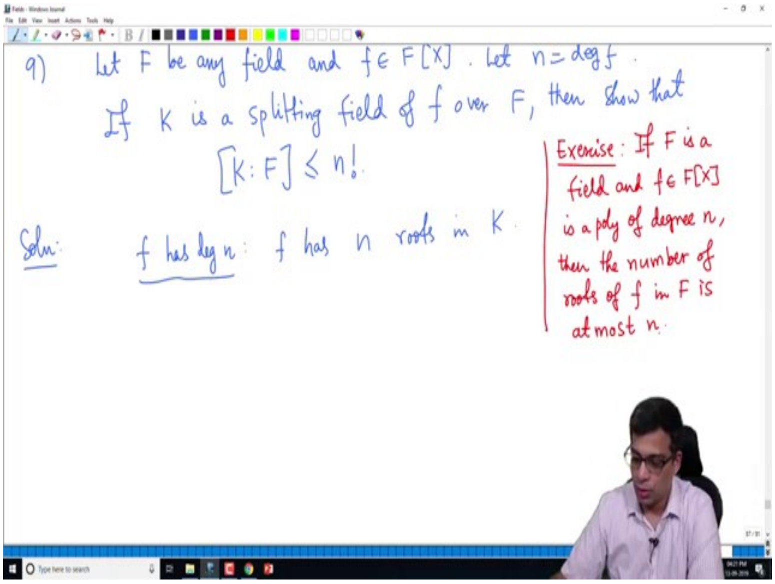
Fact: $[\mathbb{C} : \mathbb{Q}] = \infty$

Using Eisenstein criterion for example, we know that X power n plus 3 is irreducible in Q X for every n and it has no real, no and it has no rational roots. Root 3; cube root of 3 fourth root of 3 they are all not rational numbers. They can there are real numbers which are roots of this, but not rational numbers.

So, you have arbitrarily large degree polynomials, which are irreducible and which have no roots. So, this is reflected in the fact that, this I will not prove and it requires actually argument, but one can prove this and there is an exercise you can try to do this is that the extension of C over Q has infinite degree. So, you have C, R and Q this is true, but this is infinity and do so is this, ok. If this is finite of course, the whole thing will be finite. So, one way to prove that C over Q is infinities through that R over Q is infinity.

So, Q is very far from being algebraically closed. So, there are lots and lots of irreducible polynomials which have no roots, where as R is not quite algebraically closed, but it is close to being algebraically closed, ok. So, in the remainder of this lecture video, I am going to do some problems about splitting fields. So, let me get the number right. So, we have done so far 8; so, let us do 9.

(Refer Slide Time: 21:26)



9) Let F be any field and $f \in F[X]$. Let $n = \deg f$.

If K is a splitting field of f over F, then show that

$[K:F] \leq n!$

Soln: $\underline{f \text{ has deg } n}$: f has n roots in K.

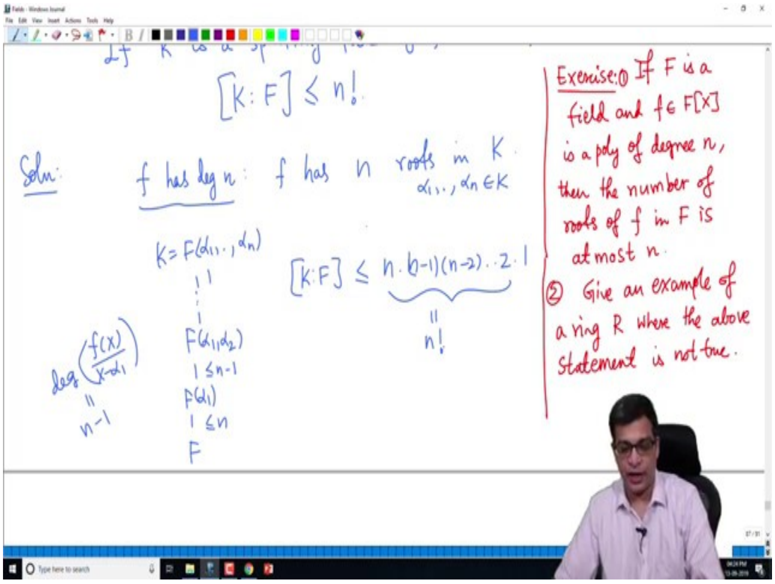
Exercise: If F is a field and $f \in F[X]$ is a poly of degree n, then the number of roots of f in F is atmost n.

So, let us now go back to an arbitrary situation. Let capital F be any field and let small f be a polynomial in capital F X ok, so this is a polynomial. Let us take s; suppose, let the degree of f be n right. If K is a splitting field of small f over capital F, then this exercise is asking you to show that, the degree is bounded by n factorial, ok.

So, this is also easy, let me quickly do the solution of this, what is the solution? So, I will sort of sketch the solution without giving you the full details. So, how do you construct the splitting field? So, f has degree n, right so, I am going to give you the worst case scenario, in other words the largest degree possible for K, right.

So, suppose f has n roots right. So, it has n roots in K and actually, I am not going to do this as an exercise, but as a problem in this video, but it is a good exercise for you to do using the theory that we developed in this course this is aside for this ok. So, I will just write this here. If F is a field and small f is a polynomial, then of degree n, then the number of roots of f in capital F is at most n. It can be maybe less than n, because it can have multiple roots. Because if you to take X minus 1 whole squared in a Q X it has only one root, but degree 2. So, but it cannot be more than 2. So, this is the first part of the exercise.

(Refer Slide Time: 23:50)



$$[K:F] \leq n!$$

Soln: f has deg n: f has n roots in K. $\alpha_1, \dots, \alpha_n \in K$

$K = F(\alpha_1, \dots, \alpha_n)$

$F(\alpha_1, \alpha_2)$ $\leq n-1$

$F(\alpha_1)$ $\leq n$

F

$\deg\left(\frac{f(x)}{x-\alpha_1}\right) = n-1$

$$[K:F] \leq \underbrace{n \cdot (n-1)(n-2) \cdots 2 \cdot 1}_{= n!}$$

Exercise: ① If F is a field and $f \in F[X]$ is a poly of degree n, then the number of roots of f in F is at most n.

② Give an example of a ring R where the above statement is not true.

Give an example of a ring which necessarily will have to be not a field where the above statement is not true, ok. So, what I am asking you to do is, give an example of a ring R and a polynomial of degree n over R which has more than n roots. So, the difference is that you can divide by the factor X minus alpha if alpha is a root here, in general you cannot divide by it ok.

So, I will not talk about this, this is a good exercise for you to do as a way of understanding both the ring theory and the field theory part of this course, ok. So, I will skip that, I will leave that as an exercise for you or you can ask questions about this in the discussion forum.

So, now coming back to this exercise we are in the case of fields. So, it can have at most n roots, degree has n suppose it has n roots in K, ok. So, let us say alpha 1, alpha 2, alpha n., because, its splits completely in capital K right, so it all the roots are there. It is possible that there are less than n roots, but then that degree of the extension will be even smaller as you will see ok.

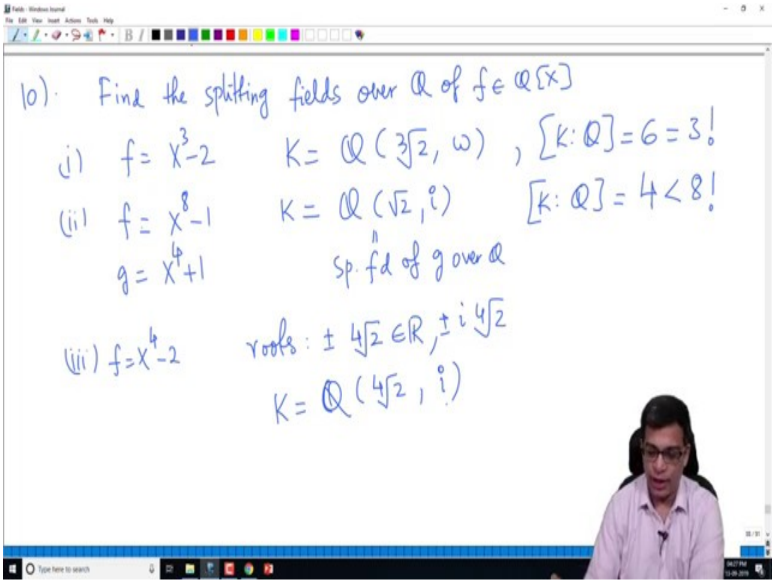
So, then what do we do is start with F, look at F alpha 1, F alpha 2 and so on, all the way to F alpha 1, alpha 2, alpha n. So, and which is our K right, because remember splitting field is a field I will write this more clearly. Splitting field is a field where the polynomial splits completely and more importantly the field is generated by those roots it is; it does not have any extra stuff above it than is needed. So, alpha 1 through alpha 1, n are the roots.

So, now, let us look at the degrees of each individual extension. I claim that degree here is less than equal to n because, alpha 1 satisfies the polynomial f right. The degree will be the degree of the irreducible polynomial, but degree of the irreducible polynomial of alpha 1 over F divides the polynomial f. So, it will have degree less than or equal to n. And here, the polynomial that alpha 2 satisfies, so this should not be alpha 2, it will be alpha 1, alpha 2; here the polynomial that alpha 2 satisfies over this will be f X divided by X minus alpha 1, because that is an element in this polynomial ring.

And this will have degree remember, is n minus 1 because F has degree n, you are removing 1 linear factor. So, this is at most degree n minus 1. It is could be smaller than that, so it is less than or equal to that and all the way to 1 you get ok. So, if you multiply this. So, the degree of K over F is less than or equal to n times n minus 1 times n minus 2 all the way up to 2 and 1, ok.

So, what I wanted to say was, yeah so, this is alright. So, this is exactly equal to n factorial ok. So, the degree is at most n factorial, it can be smaller sometimes than n factorial, but it cannot be more than n factorial. So, now, just to give you a few examples and these are problems related to splitting fields ok. So, find the splitting fields.

(Refer Slide Time: 27:44)



10). Find the splitting fields over $\mathbb{Q}$ of $f \in \mathbb{Q}[x]$

(i) $f = X^3 - 2$ $\quad K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, $[K:\mathbb{Q}] = 6 = 3!$

(ii) $f = X^8 - 1$ $\quad K = \mathbb{Q}(\sqrt{2}, i)$ $\quad [K:\mathbb{Q}] = 4 < 8!$

$g = X^4 + 1$ $\quad \overset{\shortparallel}{\text{sp. fd of } g \text{ over } \mathbb{Q}}$

(iii) $f = X^4 - 2$ $\quad$ roots : $\pm \sqrt[4]{2} \in \mathbb{R}, \pm i \sqrt[4]{2}$

$K = \mathbb{Q}(\sqrt[4]{2}, i)$

So, in the video when we talked about splitting fields, we did discuss this, but I want to just do some more examples. Find the splitting fields and I will specify all of these are over Q, ok. So, first case is something that we discussed before, X cubed minus 2.

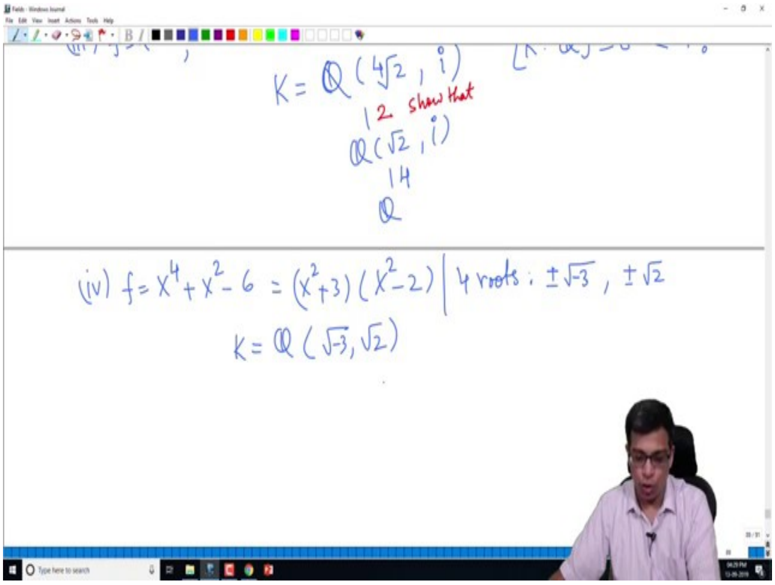
So, here the splitting field is cube root of 2 and omega, ok. So, and the extension degree is 6 which is 3 factorial, ok. So, here cube root of 2, omega cube root of 2, omega squared cube root of 2 are the roots and you can generate all of them by putting these 2 only and this is degree 6, I discussed when we discussed the splitting fields. So, this is one example where the limit the maximum value is achieved, what about f equal to X power 8 minus 1.

So, in each of these examples f is a polynomial over rational numbers, this also I claim we have essentially done, ok. So, actually the splitting field of g which is X power 4 plus 1 is equal to also the same field, because once you add i and root 2, all the other roots automatically are included there. So, I am not spending time on this because we have already discussed these in the video on splitting fields.

Here, actually if you think about it, you will only have degree 4, whereas this is much smaller than 8 factorial right. Because, here the degree is 8, so and that is just gives us an example that the actual degree can be much smaller than what n factorial is. On the other hand what is if you take X power 4 minus 2, ok.

So, here if you think about this, K will have to be so what are the roots? There will be a fourth root of 2 a real number; remember, X power 4 minus 2 is a degree 2 irreducible polynomial; degree 2 polynomial over R. So, it cannot be irreducible and in fact, it has a root, namely fourth root of 2. So, fourth root of 2 plus minus are there, two real roots and then i times fourth root of 2 plus minus are the 4 roots, and you clearly see that if you adjoin fourth root of 2 and i you get your splitting field.

(Refer Slide Time: 30:35)



$K = \mathbb{Q}(\sqrt[4]{2}, i)$

$|$ 2 show that

$\mathbb{Q}(\sqrt{2}, i)$

$|$ 4

$\mathbb{Q}$

(iv) $f = X^4 + X^2 - 6 = (X^2+3)(X^2-2)$ | 4 roots: $\pm\sqrt{-3}$, $\pm\sqrt{2}$

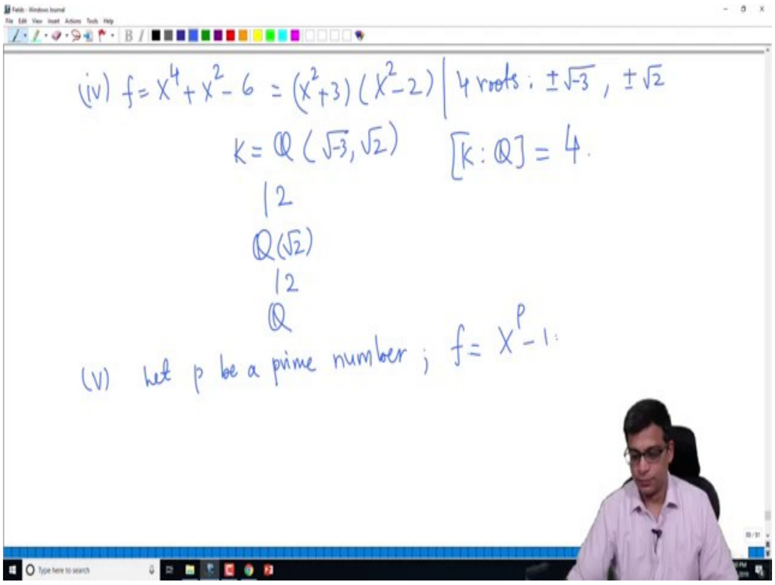
$K = \mathbb{Q}(\sqrt{-3}, \sqrt{2})$

So, this if you think for a minute is actually an extension of Q root 2, root i because, i is already there and here you are adding a square root of something that is already here, fourth root of 2 is nothing but square root of root 2. So, an exercise for you is show that this is 2, very easy exercise right, because really i is already there in both fields this whole is a field is obtained by adding a square root of root 2; that means, it is a degree two extension. And this we have seen earlier is 2 so, the total degree is 8 and which is of course, much smaller than 4 factorial ok.

So, one more; so, here smaller degree polynomial, but bigger degree of the splitting field, what about X power 4 plus X squared minus 6, ok. So, here it is a degree 4 polynomial, but if you can think about this actually splits as X squared plus 3 and X squared minus 2, right correct.

So, this is the factorization. So, the roots are root 3 plus minus because or actually X squared equals to minus root 3. So, plus minus root minus 3 and plus minus root 2 these are the 4 roots. In the earlier case also there are 4 roots because, it is degree 4 here also there are 4 roots. So, the splitting field is Q adjoined cube root of minus 3 and cube root of 2. Once you adjoined cube root of minus 3, minus cube root of minus 3 is already there, once you adjoined root 2, minus root 2 is also there.

(Refer Slide Time: 32:25)



(iv) $f = X^4 + X^2 - 6 = (X^2+3)(X^2-2)$ | 4 roots: $\pm\sqrt{-3}$, $\pm\sqrt{2}$

$$\begin{tikzcd} K = \mathbb{Q}(\sqrt{-3}, \sqrt{2}) \arrow[d, dash, "2"] \\ \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] \\ \mathbb{Q} \end{tikzcd}$$

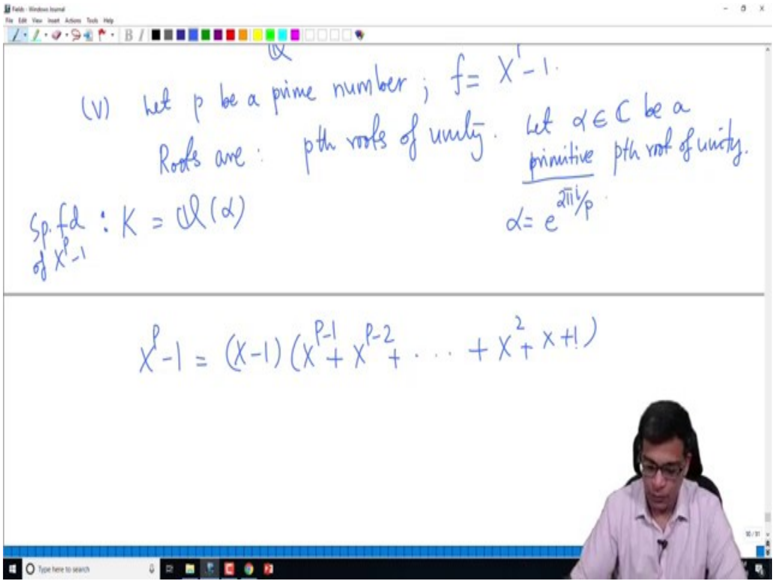
$[K:\mathbb{Q}] = 4.$

(v) Let p be a prime number; $f = X^p - 1$:

And this actually you can think construct this tower this is degree 2, this is degree 2, so K colon Q is 4.

And one final example in this; problem 5 is let p be a prime number, prime integer as always and take F to be X power p minus 1. What is the splitting field?

(Refer Slide Time: 32:55)



$\mathbb{Q}$

(V) Let p be a prime number ; $f = X^p - 1$.

Roots are : pth roots of unity. Let $\alpha \in \mathbb{C}$ be a primitive pth root of unity.

Sp. fd of $X^p - 1$: $K = \mathbb{Q}(\alpha)$

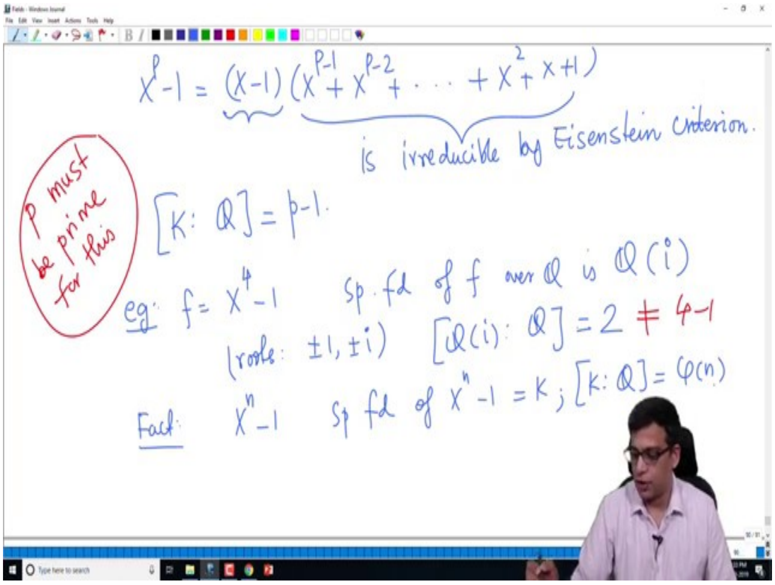
$\alpha = e^{2\pi i/p}$

$$X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1)$$

Here, we are roots are p th roots of 1. And what we observe is that because p is a prime number the degree will be p minus one. So, if you factor; so, let alpha be a primitive p th root of unity; that means, remember roots of unity form a cyclic group and a generator of that is called primitive p th root of unity.

So, all I am saying is 2 pi i by p; so, alpha can be taken as 2 pi i by p. So, the splitting field K is equal to Q adjoined alpha, right. What is the degree over Q? So the irreducible polynomial can be found out by factoring this into X power X minus 1 times X power p minus 1 plus X power p minus 2 dot dot dot X square plus X plus 1.

(Refer Slide Time: 34:10)



$$X^p - 1 = \underbrace{(X-1)}\,\underbrace{(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1)}_{\text{is irreducible by Eisenstein Criterion.}}$$

p must be prime for this

$[K:\mathbb{Q}] = p-1$.

eg: $f = X^4 - 1$ Sp. fd of f over $\mathbb{Q}$ is $\mathbb{Q}(i)$

(roots: $\pm 1, \pm i$) $[\mathbb{Q}(i):\mathbb{Q}] = 2 \neq 4-1$

Fact: $X^n - 1$ Sp fd of $X^n - 1 = K$; $[K:\mathbb{Q}] = \varphi(n)$

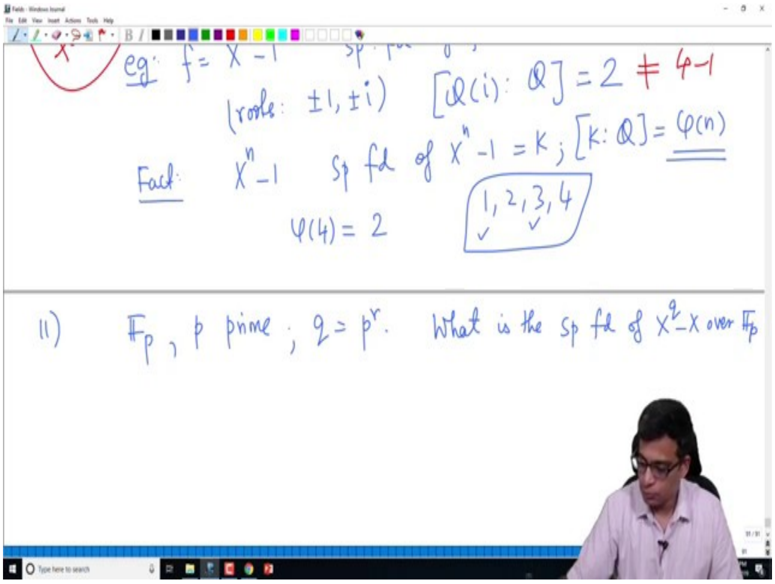
Clearly alpha is not a root of the first term, because there is only 1 root here that is 1. Alpha being a primitive p th unity certainly is not 1, because p is a prime number p is not 1. And this is irreducible if you recall from the video on Eisenstein criterion. Eisenstein criterion, it does not apply directly here, but you can modify the variable from X to X minus 1 or X plus 1 and rewrite this and apply Eisenstein criterion, so it and conclude that it is irreducible.

So, this must be the irreducible polynomial of alpha and it is degrees p minus 1, so the degree of the extension is p minus 1. So, if you adjoined the roots of X power p minus 1, p being prime is very important, because this polynomial may not be irreducible if p is not a prime, as an example.

What are the, what is the splitting field of this? Let us take X power 4 minus 1 over Q is actually Q adjoined root irreducible, sorry Q adjoined i. Because, i is a root of this, minus i roots are plus minus i, plus minus i. So, you adjoined i and you get all the other roots. And what is the degree of the extension this is actually only 2 right, in if it was it is not 4 minus 1, right. If you take the polynomial X power p minus 1, the degree is p minus 1 if p is prime, in this example shows that, if p is not prime, 4 is not prime you do not get 4 minus 1, ok.

So, you have to be a bit careful about non-primes and as a general fact you will do this in a later course sometime, the if you take X power n minus 1, the splitting field of this is K let us say. Then K colon Q is actually Euler function phi n. This is the number of integers between 1 and n that are co-prime to n; for n equal to p that is exactly p minus 1.

(Refer Slide Time: 36:42)



eg: $f = X^{} - 1$ sp fd

(roots: $\pm 1, \pm i$) $[\mathbb{Q}(i) : \mathbb{Q}] = 2 \neq 4-1$

Fact: $X^n - 1$ sp fd of $X^n - 1 = K$; $[K : \mathbb{Q}] = \underline{\underline{\varphi(n)}}$

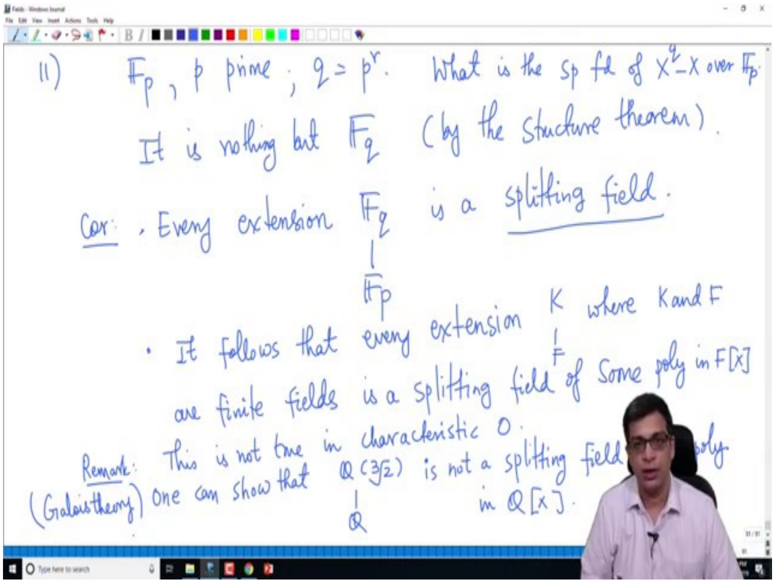
$\varphi(4) = 2$ $\boxed{\overset{}{\underset{\checkmark}{1}}, 2, \underset{\checkmark}{3}, 4}$

11) $\mathbb{F}_p$, p prime ; $q = p^r$. What is the sp fd of $X^q - X$ over $\mathbb{F}_p$

And for 4, for example you know that it is 2 because out of 1, 2, 3, 4 the co-prime ones are 1 and 3. So, they are 2, exactly 2 numbers less than 4 that are co-prime to 4. In general that is phi n, but that requires a theorem, these are, such things are called cyclotomic extensions. And as I said we are not covering everything in field theory right. Very important things are not there in this course and one of those is called cyclotomic extensions, which you learn in a more advanced course in field theory.

So, one final problem let me just to give you an example of splitting fields and characteristic p. So, let us take F p, the field with p elements, p prime, let us say q is p power R. What is a splitting field of if X power q minus X over; what is the splitting field of X power q minus X over F p, this is a very simple exercise, it is actually nothing, but F q right by the structure theorem.

(Refer Slide Time: 37:49)



11) $\mathbb{F}_p$, p prime ; $q = p^r$. What is the sp fd of $X^q - X$ over $\mathbb{F}_p$.

It is nothing but $\mathbb{F}_q$ (by the structure theorem).

Cor: . Every extension $\begin{array}{c}\mathbb{F}_q\\ |\\ \mathbb{F}_p\end{array}$ is a splitting field.

. It follows that every extension $\begin{array}{c}K\\ |\\ F\end{array}$ where K and F are finite fields is a splitting field of some poly in $F[x]$

Remark: This is not true in characteristic 0.

(Galois theory) One can show that $\begin{array}{c}\mathbb{Q}(\sqrt[3]{2})\\ |\\ \mathbb{Q}\end{array}$ is not a splitting field [illegible] poly in $\mathbb{Q}[x]$.

So, it is actually F q over it is F q. So, this is an interesting corollary of this exercise. Remember F q by the structure theorem, one of the parts in the structure theorem says that F q consists of roots of X power q minus X and every element is the root of that. So, F q is a field where this polynomial X q minus X splits completely and F q is generated by those roots.

So, it is a splitting field; that means, every extension F q over F p is a splitting field. That is a nice statement right, because every F q this argument shows that is actually a splitting field. And one can show that then every extension of finite fields, it follows that every extension K over F where K and F are finite fields is a splitting field of some polynomial, ok.

So, this requires a little bit of thinking, but the point is every arbitrary field extension where both are finite is really of the form F q contained in F q prime. And everything all both of those contain F p and F q is splitting field of some polynomial over F p by this argument. So, for the same polynomial you can take F q as a splitting field over F q prime, ok. So, this is very fast, but that is argument and such extensions are called Galois extensions and they are very important.

And final remark I will make is this is not true in characteristic 0. And this requires some additional theory, but we can show that there are lots of extensions which are not splitting field extensions. In particular for example, if you take Q adjoined cube root of 2 over Q is not a splitting field of any polynomial in Q X. It is not certainly splitting field of X cube minus 2, right. Because, X cube minus 2 by the exercise that I did here X cube minus 2 has 3 roots; cube root of 2 cube root of 2 omega cube root of 2 omega squared.

So, if you just add cube root of 2 that is not enough, this is certainly not splitting field of that particular polynomial, but I am saying something more here. It is not splitting field of any other polynomial and that requires Galois theory which is the next course that one does in fields.

So, let me end the video here and the end course also here. In this course we have studied basics of rings and fields and these are contents of a first course in abstract algebra, first course in ring theory and field theory. So, after you do some group theory, the next course that one does is rings and fields and in this 8 week course, we have covered essentially the basic notions that one learns in a first course.

In rings we have covered topics like homomorphisms of rings, quotient rings, first isomorphism theorem and we talked about UFDs, PIDs. And in fields we talked about finite extensions, algebraic extensions, transcendental extensions and splitting fields and finite fields and so on.

So, I hope you enjoyed the course; this is hopefully given you some understanding of basics of these two subjects and motivated you to learn this further and as I said there is a lot more to study in these two topics, and you should try to take more courses and learn these things more thoroughly and in advanced courses.

Thank you.