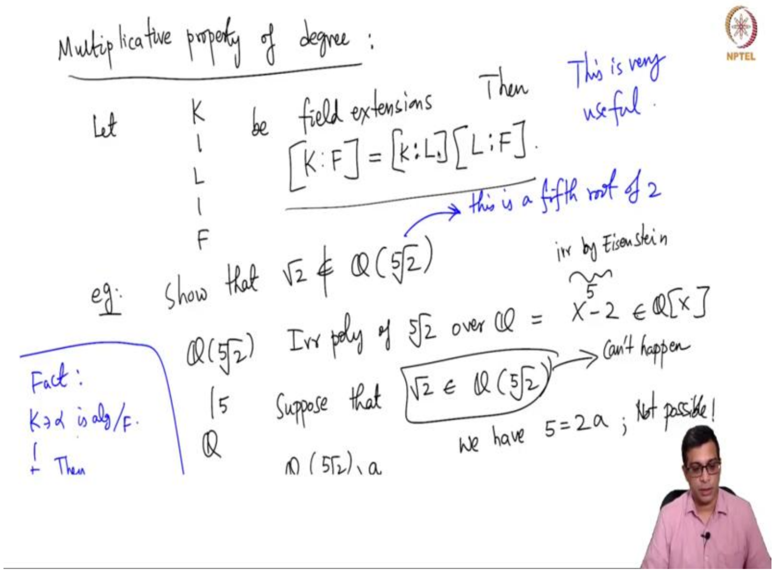
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Review of field theory – Part 2

(Refer Slide Time: 00:15)



Multiplicative property of degree :

Let $\begin{matrix} K \\ | \\ L \\ | \\ F \end{matrix}$ be field extensions Then $[K:F] = [K:L][L:F]$.

This is very useful.

this is a fifth root of 2

eg: Show that $\sqrt{2} \notin \mathbb{Q}(\sqrt[5]{2})$

irr by Eisenstein

$\begin{matrix} \mathbb{Q}(\sqrt[5]{2}) \\ |5 \\ \mathbb{Q} \end{matrix}$ Irr poly of $\sqrt[5]{2}$ over $\mathbb{Q}$ = $X^5 - 2 \in \mathbb{Q}[X]$

Suppose that $\boxed{\sqrt{2} \in \mathbb{Q}(\sqrt[5]{2})}$ → Can't happen

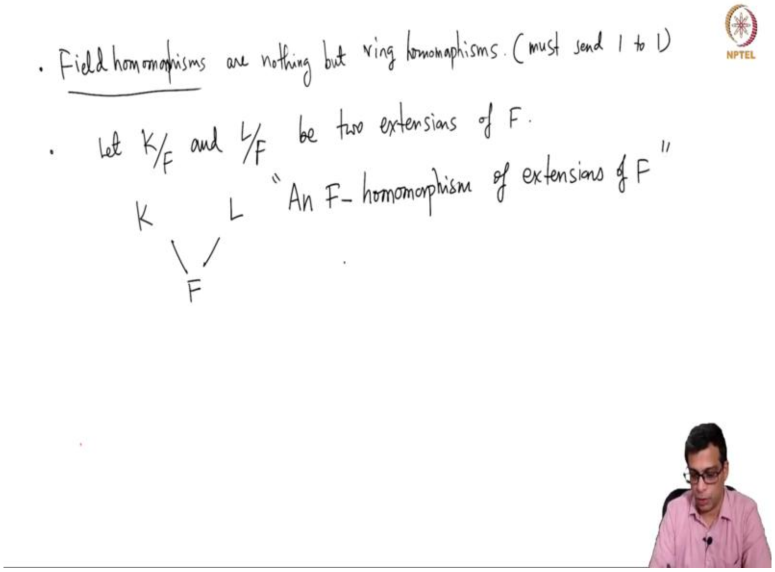
we have $5 = 2a$; Not possible!

$\mathbb{Q}(\sqrt[5]{2}) \setminus a$

Fact: $K \ni \alpha$ is alg/F.
! Then

Let us continue now. I am recalling some basic facts in field theory. And in the last video we ended with this multiplicative property of degree of field extensions. So let us continue. I will recall some other important things about field extensions.

(Refer Slide Time: 00:32)



- Field homomorphisms are nothing but ring homomorphisms. (must send 1 to 1)
- Let K/F and L/F be two extensions of F.

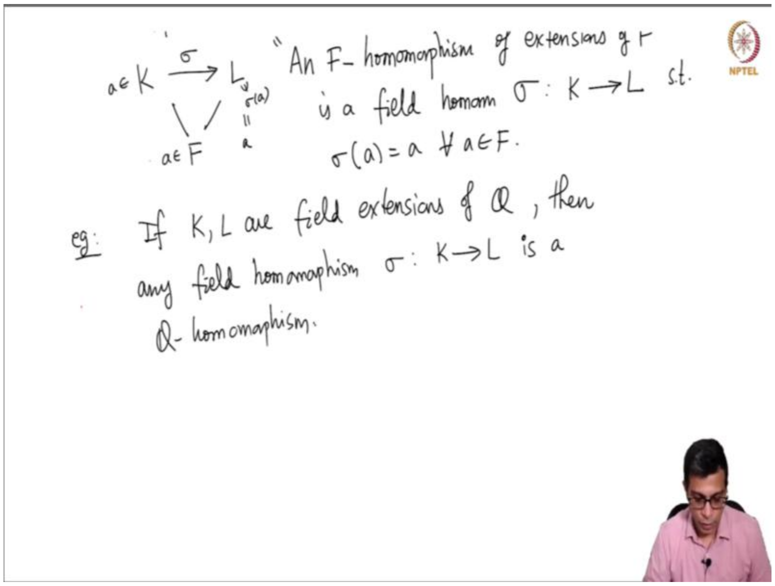
$$\begin{tikzcd} K \arrow[dr, dash] & & L \arrow[dl, dash] \\ & F & \end{tikzcd}$$

"An F-homomorphism of extensions of F"

So, let me just quickly talk about field homomorphisms first. Field homomorphisms are really nothing but ring homomorphism are nothing but ring homomorphism. So a field is a ring and a ring homomorphism is 1 which preserves the addition, multiplication of the ring and sends 1 to 1. So it must send 1 to 1. I will recall only that but there is nothing additional for a ring homomorphism that you require in order to be a field homomorphism.

What we are more interested in is the following. So let K over F and L over F be 2 extensions of F, 2 extensions of F. So you have K, L are both extensions of F. Ok we can consider homomorphisms from K to L that just completely disregards F and just reads them as 2 rings and you look at a homomorphism but an F homomorphism, an F homomorphism of extensions of F.

(Refer Slide Time: 02:04)



$$\begin{tikzcd} a \in K \arrow[rr, "\sigma"] & & L \\ & a \in F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

$\sigma(a) = a$

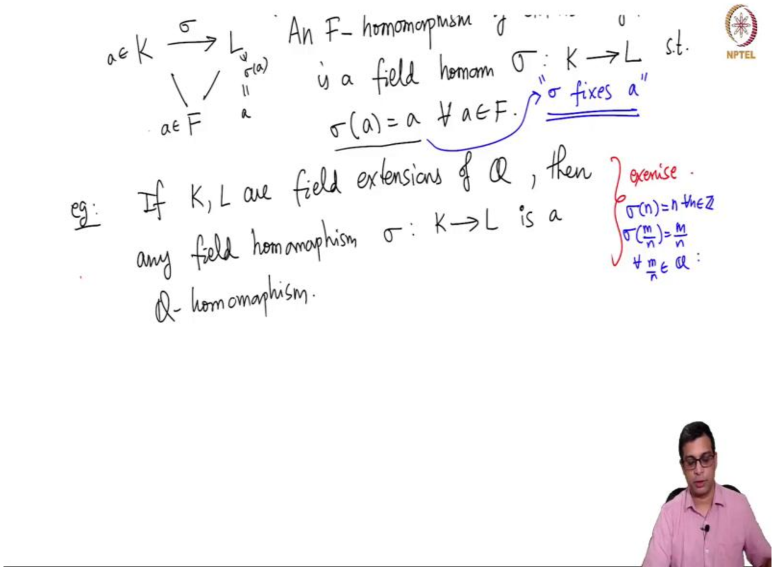
"An F-homomorphism of extensions of F is a field homom $\sigma : K \to L$ s.t. $\sigma(a) = a \ \forall a \in F$.

<u>eg:</u> If K, L are field extensions of $\mathbb{Q}$, then any field homomaphism $\sigma : K \to L$ is a $\mathbb{Q}$-homomaphism.

So if you take 2 extensions of F and you want an F homomorphism is a field homomorphism sigma from K to L. So it is a map from K to L, a field homomorphism in other words a ring homomorphism. But in order to be F homomorphism it must have further the property that sigma of A is equal to A for all A in F. Because F is a subfield of K, if A belongs to K, A belongs to F it is also an element of K. So you can ask for what is sigma is, sigma of A is an element here.

But F is a subfield of L also, so that must equally ok that is a, that is the requirement for it to be an F homomorphism. So just to give you an idea, so this is in fact an exercise for you. If K and L are field extensions of Q then any field homomorphism is a Q homomorphism.

(Refer Slide Time: 03:40)



$$\begin{tikzcd} a\in K \arrow[rr, "\sigma"] & & L \\ & a\in F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

$\sigma(a) = a$

An F- homomorphism is a field homom $\sigma: K \to L$ s.t. $\underline{\sigma(a) = a}$ $\forall a \in F$. "σ fixes a"

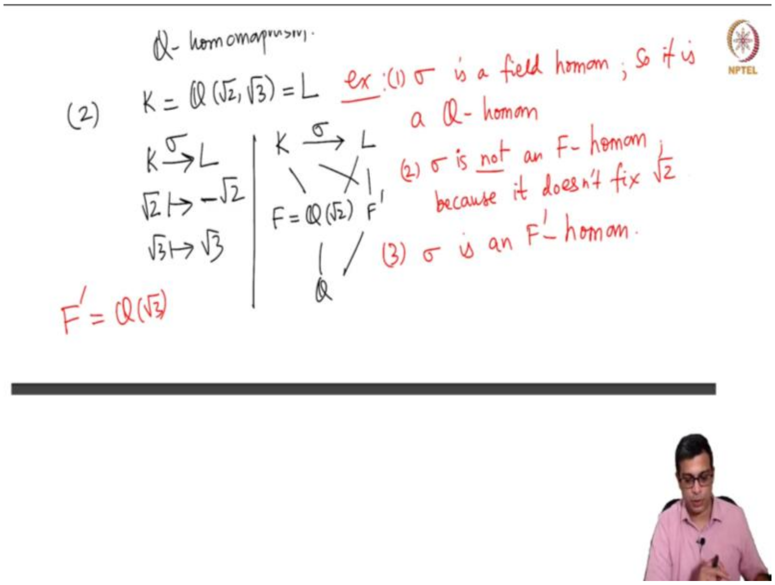
eg: If K, L are field extensions of $\mathbb{Q}$, then any field homomaphism $\sigma: K \to L$ is a $\mathbb{Q}$- homomaphism.

exercise. $\sigma(n) = n$ $\forall n \in \mathbb{Z}$, $\sigma\left(\frac{m}{n}\right) = \frac{m}{n}$ $\forall \frac{m}{n} \in \mathbb{Q}$:

So this is an important exercise. It is an important exercise for you. It says that any element of Q automatically is fixed by sigma. So that is what remember this means. So this means sigma fixes. So we will remember this condition as saying that sigma fixes. This terminology will be useful for us later. So F homomorphism must fix everything in F. So A must go to itself. So here any field homomorphism we know fixes integers.

So, actually first it fixes 1 so it fixes every integer, then it fixes this. So that is the hint. I will not go into details of this. So that is an important, so there is nothing extra for it to any homomorphism a field extensions of Q to be Q homomorphism. It is automatically a Q homomorphism.

(Refer Slide Time: 4:42)



$\mathbb{Q}$- homomorphism.

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

$K \xrightarrow{\sigma} L$

$\sqrt{2} \mapsto -\sqrt{2}$

$\sqrt{3} \mapsto \sqrt{3}$

$F' = \mathbb{Q}(\sqrt{3})$

$$\begin{tikzcd}
K \arrow[r, "\sigma"] \arrow[d, dash] \arrow[dr, dash] & L \arrow[dl, dash] \arrow[d, dash] \\
F = \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & F' \arrow[dl, dash] \\
\mathbb{Q} &
\end{tikzcd}$$

ex: (1) σ is a field homom; so it is a $\mathbb{Q}$- homom

(2) σ is not an F- homom; because it doesn't fix $\sqrt{2}$

(3) σ is an F'- homom.

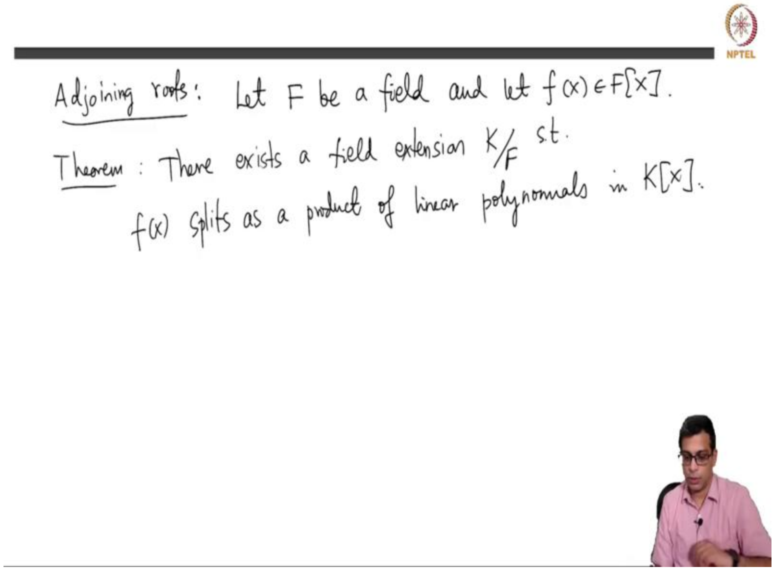
On the other hand let us take K to be Q root 2, root 3 and L to be Q root 2, root 5. So Q root 2, root 3, is the smallest subfield of let us say R containing Q root 2 and root 3. L is the smallest subfield of R containing Q and root 2 and root 5. So if you consider the map from K to L which sends root 2 to minus root 2. Sorry so here I should have, I will take K to be this itself. L to be this itself so and root 3 to root 3.

So sigma, this is an exercise for you. Sigma is a field homomorphism, so check this. This is the first exercise. So it is a Q homomorphism. Ok and note that you have K equals L. So K equals L maybe I will write this separately here. K L are sitting above Q root 2 and this is sitting over Q. So this is let us say F is this. So and this map is sigma. So that is the picture.

So this sigma is a Q homomorphism but sigma is not an F homomorphism. This is clear because it does not fix root 2. It does not fix root 2. On the other hand if I introduce a new field here F prime, so let us say F prime is equal to Q root 3. So the third exercise is a sigma is an F prime homomorphism, so F prime sits here.

They both thinks over F prime but it is an F prime homomorphism because root 3 goes to root 3. So this is just to give you an idea of what field homomorphisms are and what field homomorphisms or field extensions are.

(Refer Slide Time: 07:22)



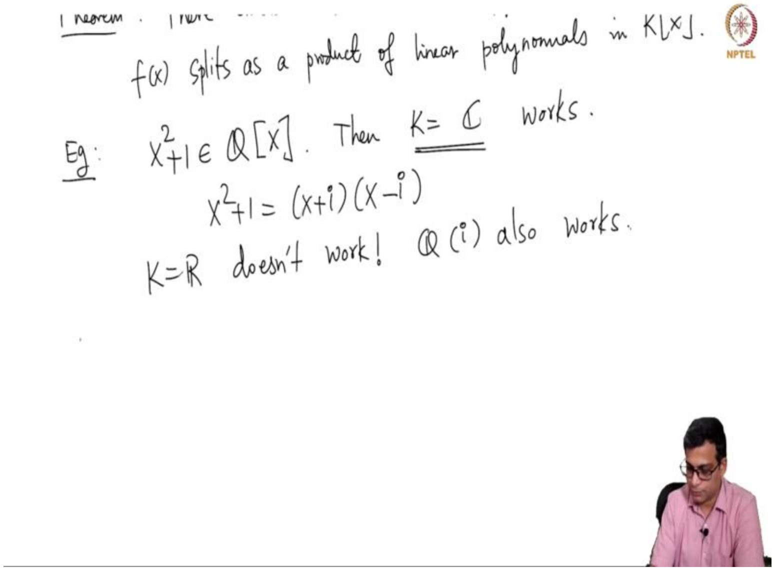
Adjoining roots: Let F be a field and let $f(x) \in F[x]$.

Theorem: There exists a field extension K/F s.t.

$f(x)$ splits as a product of linear polynomials in $K[x]$.

So now the next topic I want to discuss is very important. This is really getting to the crux of the subject in Galois theory is adjoining roots. So I am going to state a big theorem here which requires a little thinking. It is not difficult but this is done in any field theory course. So what I want to say is that let F be a field and let fx be a polynomial over that field in one variable. So the theorem is there exists a field extension K over F, K of F such that F splits as a product of linear polynomials in Kx that is all.

(Refer Slide Time: 8:31)



Theorem : There

$f(x)$ splits as a product of linear polynomials in $K[x]$.

Eg: $X^2+1 \in \mathbb{Q}[X]$. Then $\underline{\underline{K=\mathbb{C}}}$ works.

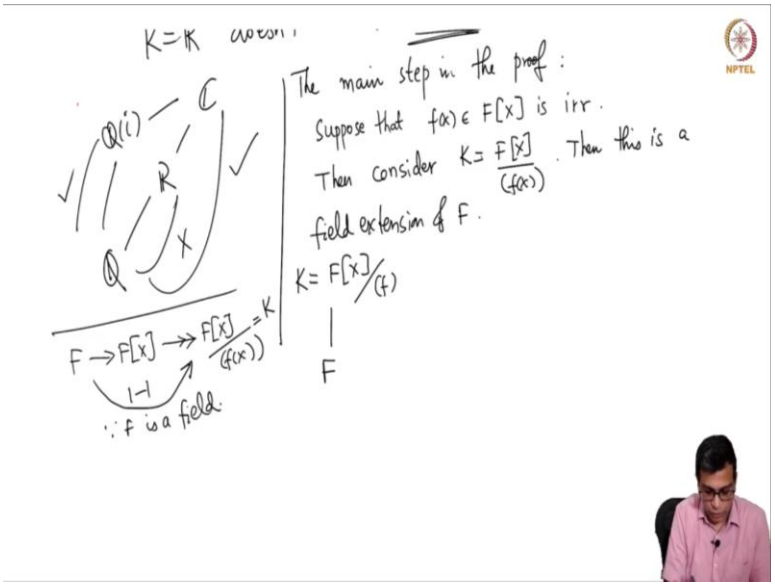
$X^2+1 = (X+i)(X-i)$

$K=\mathbb{R}$ doesn't work! $\mathbb{Q}(i)$ also works.

So the theorem is very important not difficult to prove but I will not tell you anything more than just give you a hint of how to prove this. But before that I want to introduce an important example. I mean, this is illustrate this by an example because essentially this is going to be clear if you know what, if you look at the right example.

Let us take x square plus 1 as a polynomial over Q. Then you can take K to be C because X square plus 1 does split as a product of 2 linear polynomials. K equal to C works but K equal to R does not work because X square plus 1 remains irreducible in Rx. So it does not work. You do not need to go all the way to C, Q adjoined i also works.

(Refer Slide Time: 9:34)



$$\begin{tikzcd} F \arrow[r] \arrow[rr, bend right, "1-1"'] & F[x] \arrow[r, two heads] & \frac{F[x]}{(f(x))} = K \end{tikzcd}$$

$\because F$ is a field.

The main step in the proof:
Suppose that $f(x) \in F[x]$ is irr.
Then consider $K = \frac{F[x]}{(f(x))}$. Then this is a field extension of F.

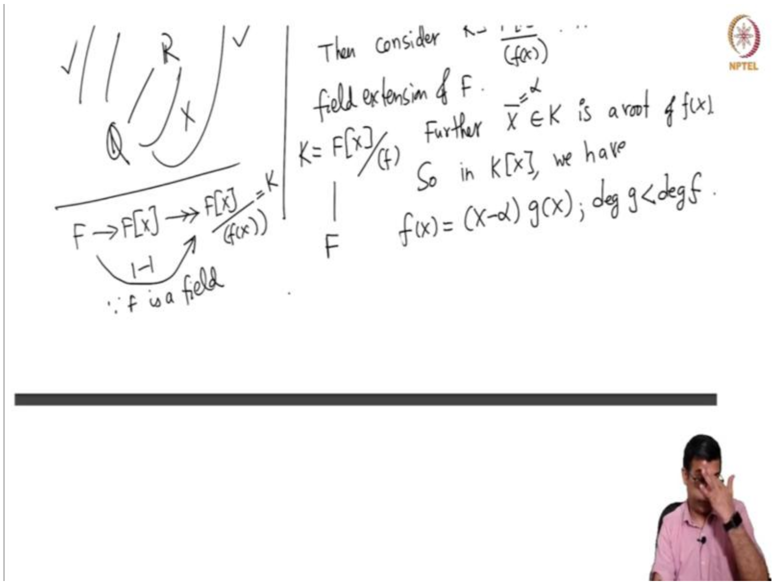
$$\begin{tikzcd} K = F[x]/(f) \arrow[d, no head] \\ F \end{tikzcd}$$

So the interesting thing is you have Q here, R here, C here does not work here. It works here. But you do not need to go all the way up to C. It is an infinite extension of Q. You can take Q adjoined i, in this it works ok. So this is the theorem is saying that there is always an extension where the polynomial splits as a product of linear polynomial means degree 1, linear means degree equal to 1 that means it has all the roots there.

X square plus 1 does not have roots in rational numbers or real numbers but it has roots in C. But in fact it also has roots in a much smaller field Q adjoined i. All the other things in C are irrelevant for this particular polynomial. You need Q adjoined i only and all I will do towards giving you idea of how to prove this theorem is the main step of the proof. So suppose F is irreducible.

Consider K to be fx modulo fx. Then this is a field extension of F. So what you have is K which is defined as fx modulo F is a field extension. This is trivial because you have F to fx and you have a subjective map by the standard properties of ring theory. And this I am calling K. So now this map is not surject not injective because there are polynomials which go to 0 namely fx itself. But this map is 1 1 because F is a field. So F is a subfield of K.

(Refer Slide Time: 11:46)



$$\begin{tikzcd} F \arrow[r] \arrow[rr, bend right, "1\text{-}1"'] & F[x] \arrow[r, two heads] & \frac{F[x]}{(f(x))} = K \end{tikzcd}$$

∵ F is a field

Then consider $K = \frac{F[x]}{(f(x))}$ . . .

field extension of F.

$K = F[x]/(f)$

$$\begin{tikzcd} K \arrow[d, dash] \\ F \end{tikzcd}$$

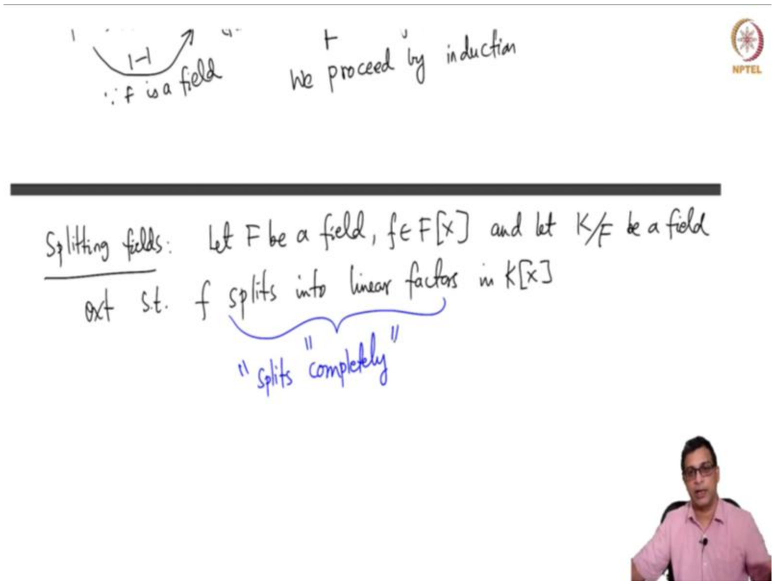
Further $\overset{=\alpha}{\overline{X}} \in K$ is a root of f(x)

So in K[x], we have

$f(x) = (X-\alpha)\, g(x)$; deg $g <$ deg f.

So this is a field extension and further X bar in K is a root of fx. Ok so we can write fx, so in Kx we have because x bar, so let me call this element let us say alpha. X bar is an element of K, so let us call that alpha. Then fx is nothing but X minus alpha times Gx and degree of G is of course strictly less that degree of F.

(Refer Slide Time: 12:26)



1-1

∵ F is a field

We proceed by induction

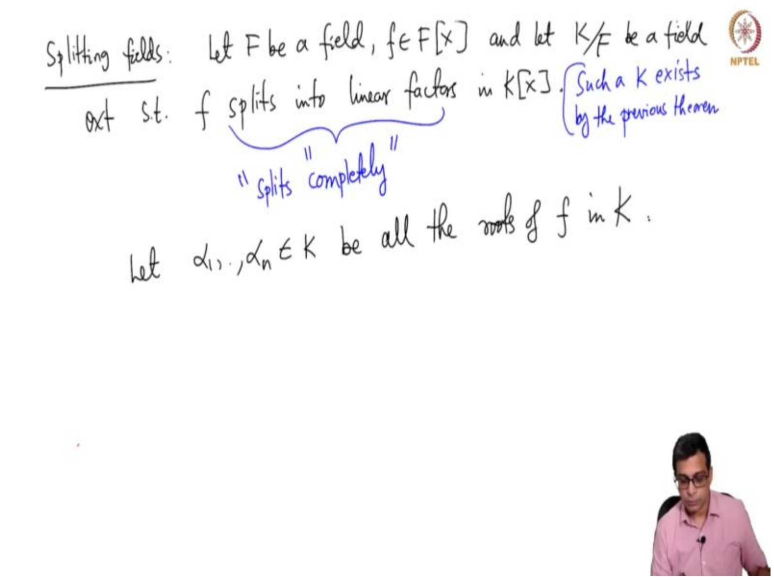
Splitting fields: Let F be a field, $f \in F[x]$ and let K/F be a field ext s.t. f $\underbrace{\text{splits into linear factors}}_{\text{"splits completely"}}$ in $K[x]$

So we proceed by induction. So we have essentially added 1 root for an irreducible polynomial. Now to prove the general statement you first look at F. You look at its irreducible factors and work with them separately 1 by 1 and once you have an irreducible factor you adjoin 1 root and then you reduce the degree so you can proceed by induction.

So this is a very important theorem that will be essential in Galois theory. Now I am going to introduce this very important notion of splitting fields which is related to the field K that we constructed above. So this is the following. So let F be a field. So let F be a field and let us take a polynomial in capital fx and let K be a field extension such that F split into linear factors in Kx.

Ok so just to avoid writing this entire sentence here, splits into linear factors, I will express that as splits completely, splits completely means you can write if F has degree 10 then there will be 10 linear factors, may be repeating but there will be 10 linear factors.

(Refer Slide Time: 14:01)

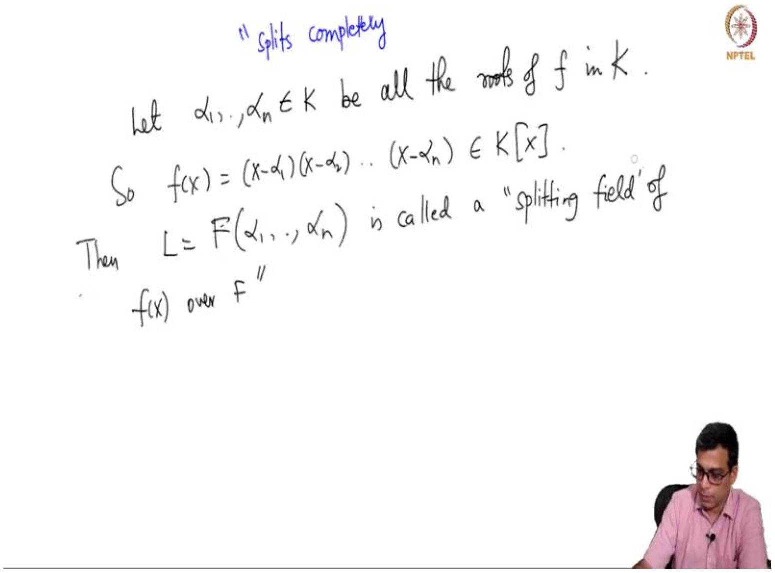


Splitting fields: Let F be a field, $f \in F[x]$ and let K/F be a field ext s.t. f $\underbrace{\text{splits into linear factors}}_{\text{" splits "completely"}}$ in $K[x]$. Such a K exists by the previous theorem

Let $\alpha_1, .., \alpha_n \in K$ be all the roots of f in K.

So now such a K exists by the previous theorem, such a K exists by the previous theorem. Now as this example here of C for x square plus 1 showed, maybe we are doing too much in that field, maybe there are lots of field, lots of unnecessary elements and we do not need those. So this is the following, so now a splitting field. So before I define that, so let us say let alpha 1 to alpha r, alpha n let us say be all the roots of f in K.

(Refer Slide Time: 14:56)



" splits completely

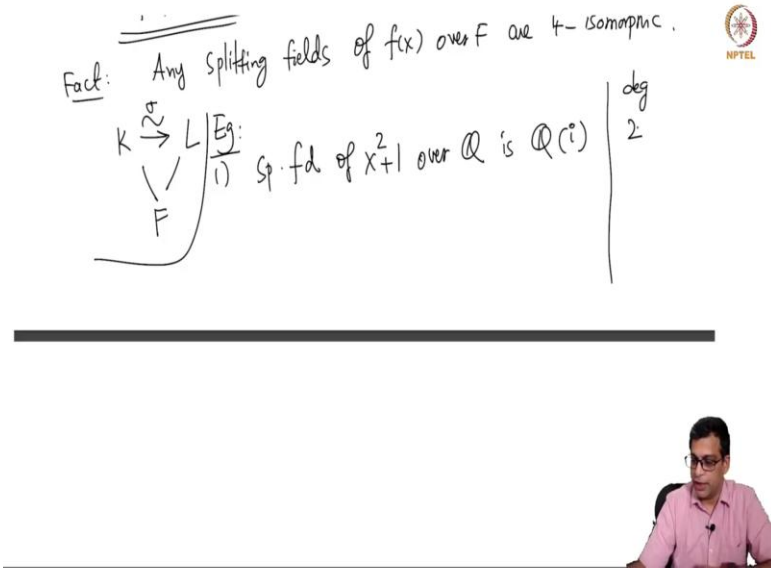
Let $\alpha_1, .., \alpha_n \in K$ be all the roots of f in K.

So $f(x) = (x-\alpha_1)(x-\alpha_2) .. (x-\alpha_n) \in K[x]$.

Then $L = F(\alpha_1, .., \alpha_n)$ is called a "splitting field' of $f(x)$ over F"

In other words what we are saying is that fx splits completely as X minus alpha 1, X minus alpha 2 times X minus alpha n. And this holds only in Kx. So then the subfield F adjoined alpha 1 to alpha r are clearly algebraic. So I can use square bracket or round bracket is called a splitting field. So the full sentence is important splitting field of fx over F.

(Refer Slide Time: 15:40)



Fact: Any splitting fields of $f(x)$ over F are F- isomorphic.

$$\begin{tikzcd} K \arrow[rr, "\overset{\sigma}{\sim}"] & & L \\ & F \arrow[ul, no head] \arrow[ur, no head] & \end{tikzcd}$$

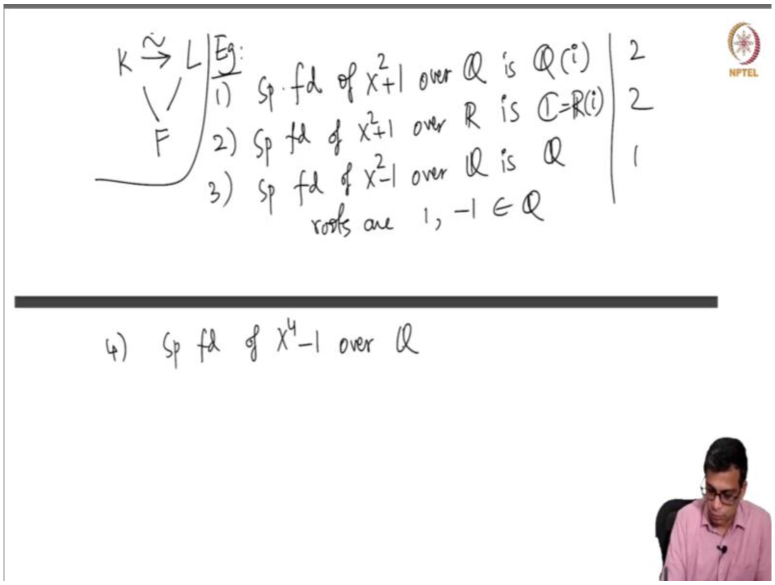
Eg:

1) Sp. fd of x^2+1 over $\mathbb{Q}$ is $\mathbb{Q}(i)$ | deg 2.

Splitting field of fx over F. So just take the smallest field containing all the roots then it is called the splitting field. And then there is a fact, which is that any 2 splitting fields K any split of a polynomial fx over F are F isomorphic. Not only are they isomorphic not only are they isomorphic as F extensions but there sorry not only are they isomorphic as fields, they are isomorphic as F extensions.

So that means if K and L are 2 splitting fields then there is an isomorphism as F extensions of F that means there is an isomorphism of fields which fixes every element of F. Ok let me quickly give you some examples. So obviously splitting field so maybe I will write yea, so examples splitting fields, I am going to write this as sp dot fd in short of x square plus 1 over Q is Q adjoined i. So and I will write degree here, degree of the splitting field is 2.

(Refer Slide Time: 17:18)



$$\begin{tikzcd} K \arrow[rr, "\sim"] \arrow[dr, dash] & & L \arrow[dl, dash] \\ & F & \end{tikzcd}$$

Eg:

1) Sp. fd of x^2+1 over $\mathbb{Q}$ is $\mathbb{Q}(i)$ | 2

2) Sp fd of x^2+1 over $\mathbb{R}$ is $\mathbb{C}=\mathbb{R}(i)$ | 2

3) Sp fd of x^2-1 over $\mathbb{Q}$ is $\mathbb{Q}$ | 1

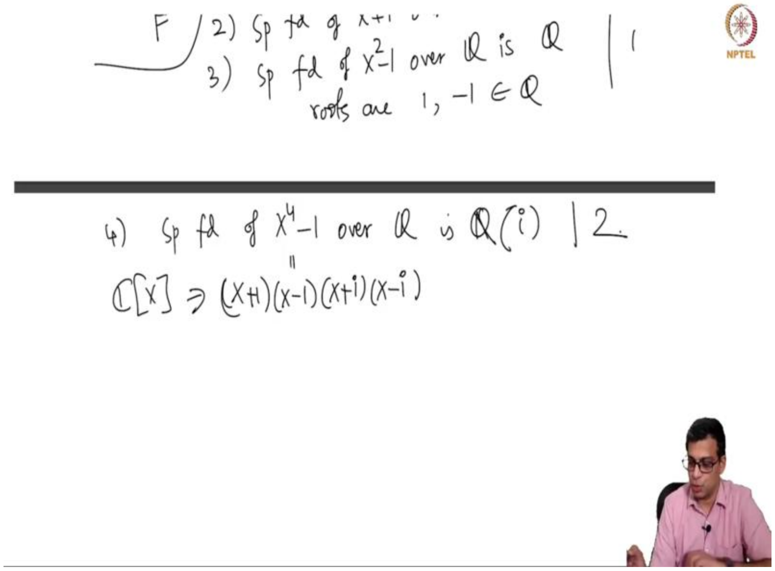
roots are $1, -1 \in \mathbb{Q}$

4) Sp fd of x^4-1 over $\mathbb{Q}$

So splitting field of x square plus 1 over Q is Qi because you can take C where the polynomial splits completely and you just adjoin the roots, which are i and minus i. So adjoining i is enough. What is the splitting field of X square plus 1 over R? Actually this is nothing but see this is R adjoined i.

So the degree is still 2.What is the splitting field of x square minus 1 over Q? This is actually just Q itself and the degree is 1 because here roots are 1 and minus 1. They are all already in Q. So you do not need to add anything more. What is the splitting field of x4 minus 1 over Q?

(Refer Slide Time: 18:00)



F / 2) Sp fd of $X+1$ ...

3) Sp fd of X^2-1 over $\mathbb{Q}$ is $\mathbb{Q}$ | 1

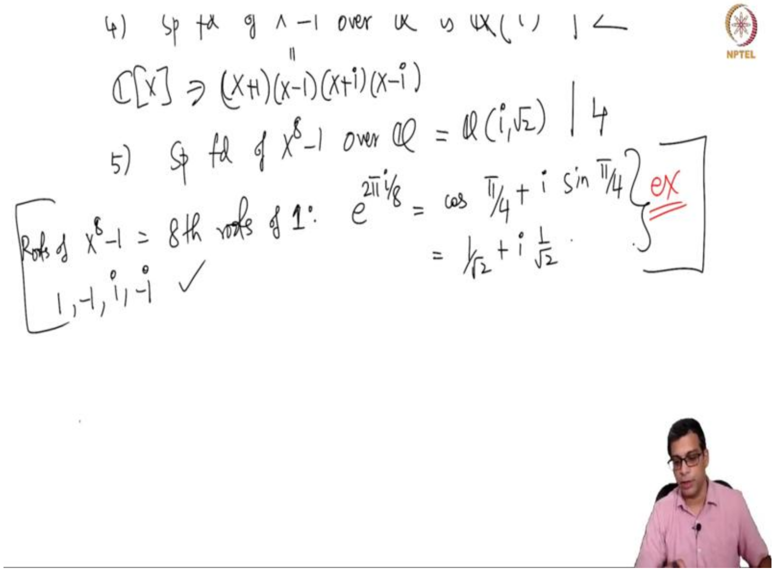
roots are $1, -1 \in \mathbb{Q}$

4) Sp fd of X^4-1 over $\mathbb{Q}$ is $\mathbb{Q}(i)$ | 2.

$\mathbb{C}[X] \ni \overset{\parallel}{(X+1)(X-1)}(X+i)(X-i)$

So in order to do this we have to figure out how this splits. This split as X plus 1, X minus 1, X plus i, X minus i, this inside Cx. In Cx this is how it splits, 1 is, 1 and minus 1 are already in Q. So if we adjoined i, minus i will already be there. So this is Q adjoined i as before, so the degree is 2 here also.

(Refer Slide Time: 18:34)



4) Sp fd of X^4-1 over $\mathbb{Q}$ is $\mathbb{Q}(i)$ | 2

$\mathbb{C}[X] \ni \overset{\parallel}{(X+1)(X-1)}(X+i)(X-i)$

5) Sp fd of X^8-1 over $\mathbb{Q}$ $= \mathbb{Q}(i,\sqrt{2})$ | 4

Roots of X^8-1 = 8th roots of 1: $e^{2\pi i/8} = \cos \pi/4 + i \sin \pi/4 = 1/\sqrt{2} + i\frac{1}{\sqrt{2}}$ ex

$1, -1, i, -i$ ✓

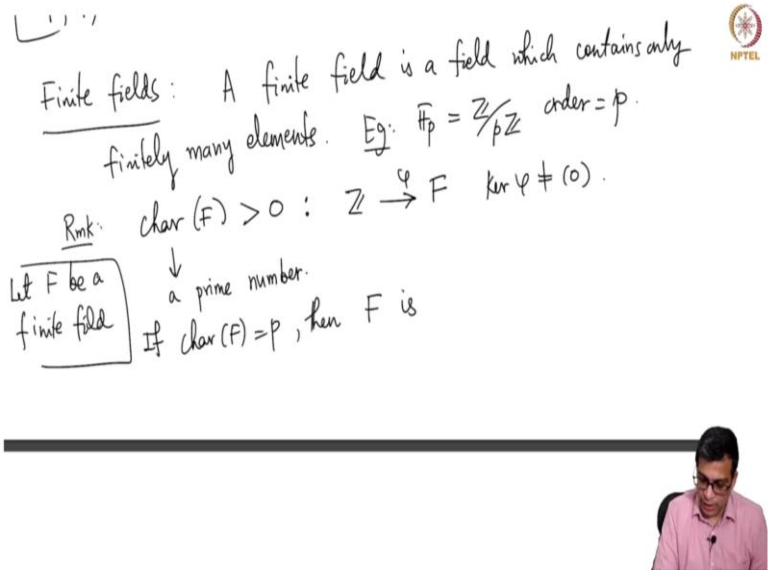
And finally I will do 1 example. This requires a bit more thinking. What is the splitting field of x power 8 minus 1 over Q? So here x power 8 minus 1 splits as, I mean these are the roots of this are 8th roots of 1. So clearly 1, minus 1, i, minus i will be there but there are more. And this is some complex number if you know these are the elements on the circle, so these are primitive, this is a primitive nth root of, 8th root of unity.

And this if you recall the formula, this is cosine pi by 4 plus i sin pi by 4. So this is 1 over root 2 plus i times 1 over root. Ok so now you can check that if you adjoined i already. So 1 over root 2 will be there. So i one can check that 1 root 2 will be there. So the splitting field is just i comma root.

Ok so this is this part is an exercise for you. So the splitting field is exactly 1 over sorry Q adjoined i comma root 2 and the degree is 4 here. So the degree of the splitting field is 4. So as you can see degree is something smaller than the, the degree of the splitting field is some number which is less than or equal to the degree of the polynomial.

Here degree of the polynomial happens to be equal to the degree of the splitting field. Here degree of the polynomial is strictly more than the degree of the splitting field and so is this in this examples. Ok so the entire Galois theory is really about studying splitting fields. So I am going to when I start proper Galois theory next time I am going to spend a little bit more time on splitting fields and introduce new concepts there.

(Refer Slide Time: 20:42)



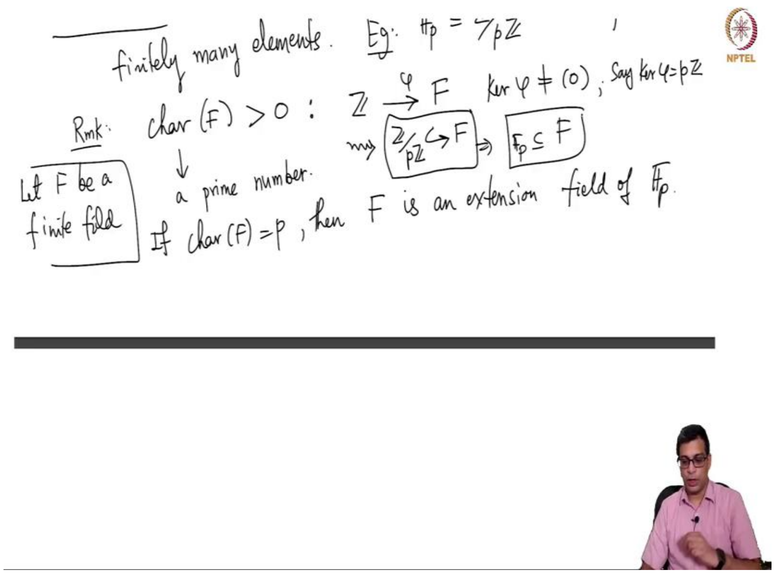
Finite fields: A finite field is a field which contains only finitely many elements. Eg: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ order $= p$.

Rmk: $\mathrm{char}(F) > 0$: $\mathbb{Z} \xrightarrow{\varphi} F$ $\ker\varphi \neq (0)$.

↓ a prime number.

Let F be a finite field

If $\mathrm{char}(F) = p$, then F is



finitely many elements. Eg: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Rmk: $\text{char}(F) > 0$: $\mathbb{Z} \xrightarrow{\varphi} F$ $\ker\varphi \neq (0)$; Say $\ker\varphi = p\mathbb{Z}$

$\rightsquigarrow \boxed{\mathbb{Z}/p\mathbb{Z} \hookrightarrow F} \Rightarrow \boxed{\mathbb{F}_p \subseteq F}$

$\downarrow$ a prime number.

Let F be a finite field

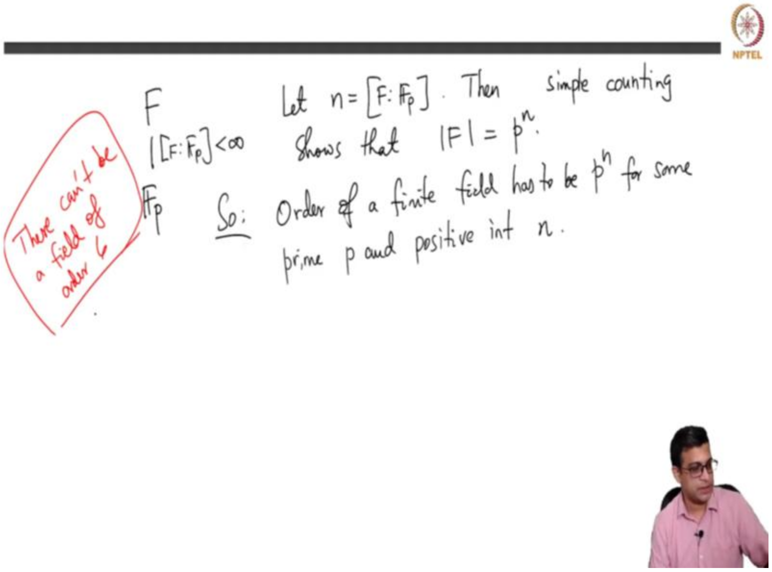
If $\text{char}(F) = p$, then F is an extension field of $\mathbb{F}_p$.

So, this is just to give you a basic idea of the definitions of splitting fields. And the final topic that I want to do in the review is finite fields, talk a little bit about structure of finite fields. Ok so a finite field, as the name suggests is a field which contains only finitely many elements. So the primary example for us is FP, which is by definition Z not PZ. The order here is P.

So, the some important observations about finite fields, characteristic of a finite field is greater than 0 because remember I recalled the characteristic. You have a if F is a finite field, so let F be a finite field. In this rest of this video F is a finite field. There is a homomorphism the kernel has to be non-zero because if the kernel is 0, Z will be contained in F, Z is infinite so F will be infinite.

But F is finite so kernel will be non-zero. It is generated by a prime number then. So characteristic is in fact a prime number. And in for, if characteristic further we have, if characteristic of F is P let us say then F is an extension of Z mod. So let me write as FP because that is clear because the kernel say kernel is PZ. So this gives me my isomorphism theorem in rings an inclusion like this. And this is nothing but FP. So F is an extension field of FP.

(Refer Slide Time: 23:10)



F

$|[F:\mathbb{F}_p]<\infty$

$\mathbb{F}_p$

Let $n=[F:\mathbb{F}_p]$. Then simple counting shows that $|F|=p^n$.

So: Order of a finite field has to be p^n for some prime p and positive int n.

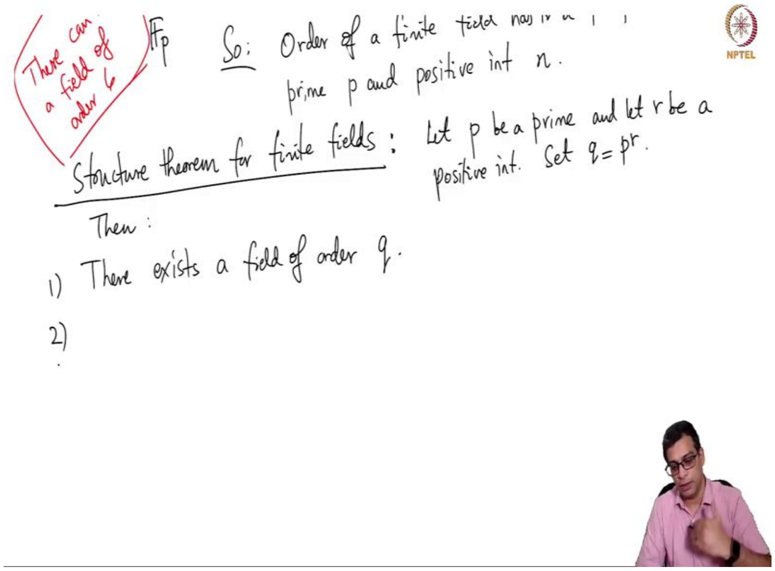
There can't be a field of order 6.

So now if you look at this, this degree is going to be finite, obviously because F itself is a finite site, so there is a finite basis. So this is a finite extension. So let us say n is the degree. Then a simple counting computation calculation shows that, then simple counting shows that cardinality of F is actually P power n because there is a basis consisting of n elements, so all elements of F can be obtained by putting some coefficients in front of the basis.

So, for each basis element you have n sorry P possibilities because the coefficients have to come from FP. So there are P possibilities for the 1st basis, P for the 2nd basis, P for the 3rd basis element, P for the nth basis element. So altogether you have P times P times Pn times namely P power n elements. So in conclusion a finite card, order of a finite field has to be P power n for some prime P and positive integer n.

So, in particular they cannot be a field of order 6 because 6 is not a power of a prime number. You have to take a single prime whereas it can possibly be 8 or 9 or 16 or 25. So we do not we have only showed that if you are given a finite field its order must be P power n. Now the question is given P power n is there a field of order P power n?

(Refer Slide Time: 25:10)



There can't a field of order 6

$\mathbb{F}_p$

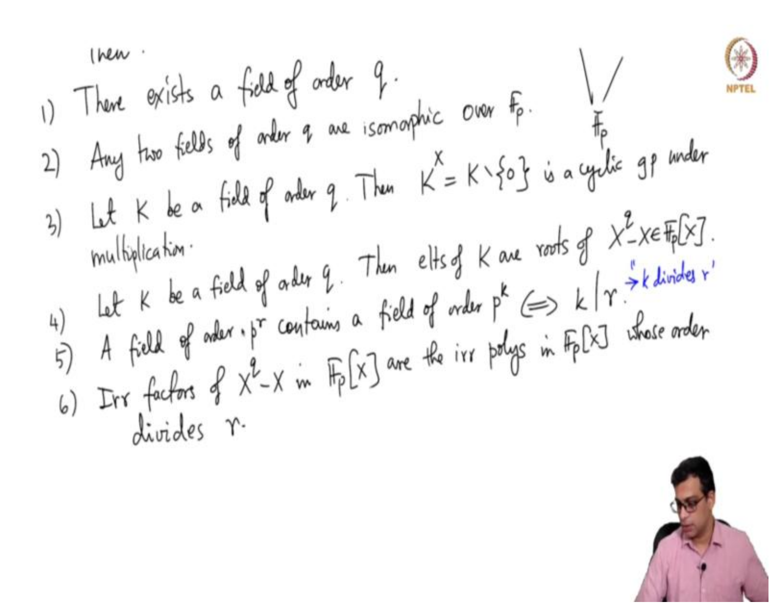
So: Order of a finite field has to be p^n for some prime p and positive int n.

Structure theorem for finite fields: Let p be a prime and let r be a positive int. Set $q = p^r$.

Then:

1) There exists a field of order q.

2)



Then:

1) There exists a field of order q.

2) Any two fields of order q are isomorphic over $\mathbb{F}_p$.

3) Let K be a field of order q. Then $K^{\times} = K \setminus \{0\}$ is a cyclic gp under multiplication.

4) Let K be a field of order q. Then elts of K are roots of $X^q - X \in \mathbb{F}_p[X]$.

5) A field of order p^r contains a field of order $p^k \iff k \mid r$. → "k divides r"

6) Irr factors of $X^q - X$ in $\mathbb{F}_p[X]$ are the irr polys in $\mathbb{F}_p[X]$ whose order divides r.

And this is expressed in this structure theorem of, so I am going to write a series of facts about finite fields. One of them answers the question that I just raised. We may not need all of this, but I thought it would be good idea for you to recall them before we embark on the study of Galois theory. So let m, P be a prime number and let r, I am going to use r here, be a positive integer. Set Q to be P power R. So then the following hold. The first statement is there exists a field of order Q.

So this answers the question, give me any prime number power positive integer there is a field of order Q that means there is a field of order 4, there is field of order 8, there is field of order 16, there is a field of order 9, 27 and so on. Moreover any 2 fields of order Q are isomorphic, in fact over FP. They are isomorphic over FP so they are both extensions as I said, any 2 fields over, any 2 fields of order Q are extensions of FP.

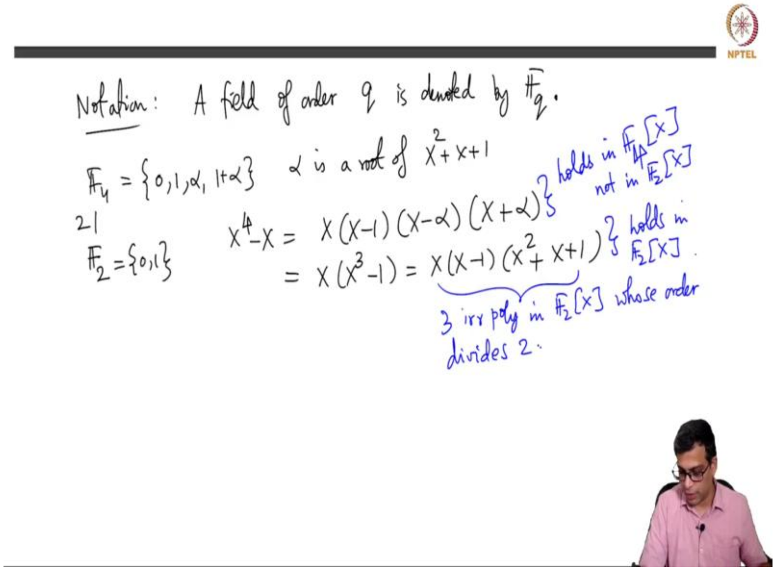
There is an isomorphism like this. So let K be a field of order Q then the collection of non-zero elements of K, K cross is a cyclic group under of course the multiplication operation, which is this is a very useful statement that we might at some point use. Let K be a field of order Q then elements of K are roots of. So K is in fact the splitting field of this polynomial X power Q minus X over FP. It is very rare that roots of a polynomial form a field or even a group.

It just happens that the roots of this particular polynomial form a field of order Q. There are Q elements its degree Q, they are all distinct one has to prove that and they form a field. That is in fact how you construct a field x, a field of order Q. So a field of order P power R contains a field of order P power K, if and only if K divides R.

Ok this symbol, remember means that K divides R. This is my short hand for K divides R. So only way that P power R contains a field of order P power K is K divides R. I will give you an example of this in a minute. And finally this might be useful for us later.

Irreducible factors of x power Q minus x in F fpx are the irreducible polynomial in fpx whose order divides R. Ok so this may not I mean you recall this that is good otherwise you should go back and check this, proof of this theorem. But these are the 6 facts that we learn about finite fields.

(Refer Slide Time: 29:21)



Notation: A field of order q is denoted by $\mathbb{F}_q$.

$\mathbb{F}_4 = \{0,1,\alpha,1+\alpha\}$ α is a root of X^2+X+1

$2|$

$\mathbb{F}_2 = \{0,1\}$

$X^4 - X = X(X-1)(X-\alpha)(X+\alpha)\}$ holds in $\mathbb{F}_4[X]$ not in $\mathbb{F}_2[X]$

$= X(X^3-1) = \underbrace{X(X-1)(X^2+X+1)}\}$ holds in $\mathbb{F}_2[X]$.

3 irr poly in $\mathbb{F}_2[X]$ whose order divides 2.

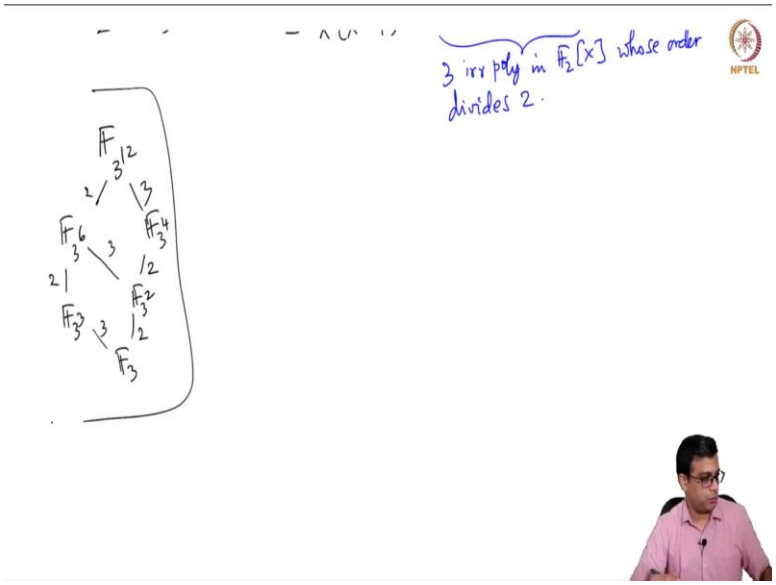
So, just to give you an idea, so example, how to construct a field of order 4? So notation is that, for convenience, a field of order Q is denoted by, this agrees with our notation of FP and it also is meaningful because any 2 fields are isomorphic so we are permitted to use a single notation for any field of order Q.

So up to isomorphism it is 1 only. So a field of order Q is denoted by fq. So now what is F4? So F4 must be an extension of degree 2 because a number of elements of F4 will be 2 power 2. So this is a degree 2 extension and if you, 0 and 1 are there always, of course because 0 and 1 are here, but the new elements can be denoted by alpha and 1 plus alpha or 1 minus alpha where alpha is a root of X power X square plus X plus 1.

This is the only reducible polynomial of degree 2 in F2x. So that means elements of F alpha can be represented as roots of the thread because this is X times X minus 1 times x minus alpha times X plus alpha. I mean, this is how it is. But we factor this usually as first you do X times x cube minus 1, then you do X times X minus 1 times X square plus x plus 1. Ok this so I should really write this holds in F4x not in F2x because alpha is not in F2.

This holds in F2x and the point is these are the 3 irreducible polynomials in F2x whose order divides 2, that is the last sentence. The irreducible factors of x power Q minus x or in this case x power 4 minus x in F2x are the irreducible polynomials whose order divides R in this case 2. So and then the final example about the series of inclusions.

(Refer Slide Time: 32:02)


3 irr poly in $\mathbb{F}_2[x]$ whose order divides 2.

So, if you take a field of order 3 power 12. So it contains a field of order 3 power 6 because 6 divides 12, it contains a field of order 3 power 3 and this contains F3. On the other hand, you have also F3 power 4, but there is no relation between F3 power 6 and F3 power 4 because 4 does not divide 6. So you also have F3 square is contained F3 4. F3 square is also contained in F3 6 because 2 divides 6.

So, there is any bar here represents an inclusion represents a field extension. There is no bar. I mean R is series of bars from 2 to 12 there is series of bars, from 2 to 6 there is a bar, but 2 to 3 there is no bar because 2 does not divide 3. And if you want to write the degrees here, this will be degree 2, this will be also degree 2 because 3 square to that, this will be degree 4 and the entire degree of course is 12, 2 times 2 times 12, which we know.

So, this degree will be 2, this degree will be 3 and this degree will be 3. So you can go from F3 to F3 power 6, either like this which is 2 times 3, sorry. And this is 2 I should write. So 3 times 2 like this or 2 times 3 like this. So this is just a tree of subfields of F3 power 12. Ok so let me stop this video here. This more or less completes the revision that I wanted to do. And from the next video we will start our study of Galois Theory. Thank you.