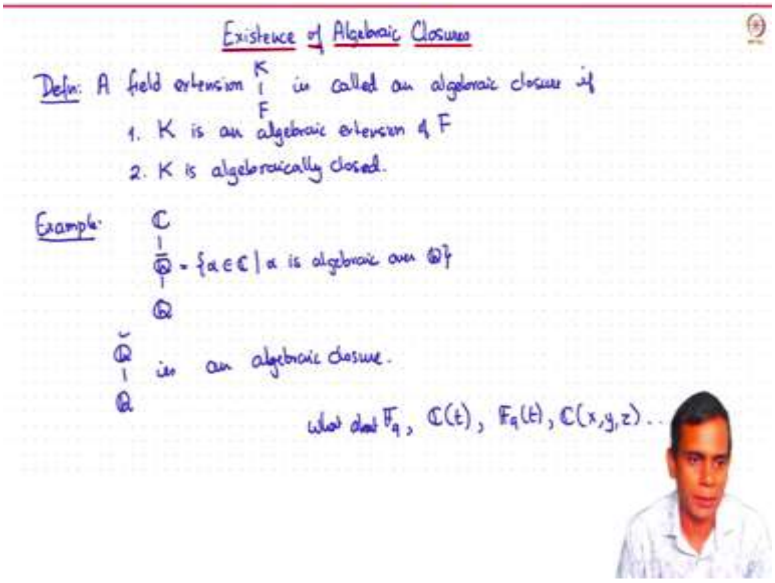
Algebra II
Professor – Amritanshu Prasad
The Institute of Mathematical Sciences
Existence of Algebraic Closures

(Refer Slide Time: 00:20)



Existence of Algebraic Closures

Defn: A field extension $\begin{matrix} K \\ | \\ F \end{matrix}$ is called an algebraic closure if

1. K is an algebraic extension of F
2. K is algebraically closed.

Example: $\begin{matrix} \mathbb{C} \\ | \\ \bar{\mathbb{Q}} \\ | \\ \mathbb{Q} \end{matrix}$ $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$

$\begin{matrix} \bar{\mathbb{Q}} \\ | \\ \mathbb{Q} \end{matrix}$ is an algebraic closure.

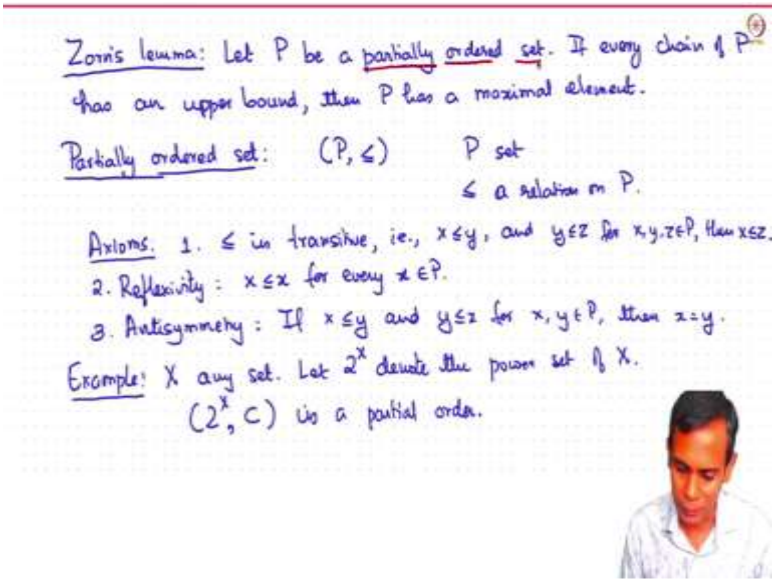
what about $\mathbb{F}_q$, $\mathbb{C}(t)$, $\mathbb{F}_q(t)$, $\mathbb{C}(x,y,z)$ . .

In this lecture, we are going to prove the existence of algebraic closures. We begin with the definition of an algebraic closure. A field extension K over F is called an algebraic closure, if a two conditions are satisfied. The first is that, K is an algebraic extension of F. And the second condition is that, K is algebraically closed.

In this case we call K an algebraic closure of F. We have already seen an example of an algebraic closure. We have the complex numbers containing the rational numbers. And in between we have Q bar, which we defined to be those complex numbers, which are algebraic over Q. And we have seen that Q bar over Q is an algebraic closure.

In the case of the rational numbers, we were lucky to have this field of complex numbers to work with. But what about fields like finite field, Fq with Q elements? Or what about a field like rational functions with say complex coefficients or rational functions with coefficients in a finite field? Or fields with multiple, rational functions in multiple variables? Each of these fields it turns out, admits an algebraic closure.

(Refer Slide Time: 02:50)



Zorn's lemma: Let P be a partially ordered set. If every chain of P has an upper bound, then P has a maximal element.

Partially ordered set: $(P, \leq)$ P set

$\leq$ a relation on P.

Axioms. 1. $\leq$ in transitive, ie., $x \leq y$, and $y \leq z$ for $x, y, z \in P$, then $x \leq z$.

2. Reflexivity : $x \leq x$ for every $x \in P$.

3. Antisymmetry : If $x \leq y$ and $y \leq z$ for $x, y \in P$, then $x = y$.

Example: X any set. Let 2^X denote the power set of X.

$(2^X, \subset)$ is a partial order.

And what I am going to show you in this lecture is a proof that every field admits an algebraic closure. Now, the proof uses a very deep axiom of mathematics called Zorn's lemma. So, let us talk about Zorn's lemma. I will state Zorn's lemma first, and then we will carefully go over the meaning of each of the terms that appears in the statement.

So, Zorn's lemma says that if you have a partially ordered set P, where every chain has an upper bound, then P has a maximal element. So, that is the statement. Let us now break it down and see what each of these terms that occur in the, in the statement means. So, to begin with, let us talk about partially ordered sets.

What is a partially ordered set? A partially ordered set is a set up together with a relation less than or equal to, we call it less than or equal to, it is a partial order relation. So, P is a set and this is a relation on P. And it must satisfy the following axioms. The first axiom is, the axiom of transitivity; which means that if x is less than or equal to y, and y is less than or equal to say, for x, y, z in P then x is less than or equal to say z.

So, this is a property that we are familiar with that the order in real numbers or integers satisfies. And the second property is called reflexivity. So, reflexivity and it says that x is less than or equal to x for every x in P. And the third property is called antisymmetry, which says that, if x is less than or equal to y, and y is less than or equal to x, for any x, y in p, then x must be equal to y.

So, these three properties are all properties that you are familiar with the natural numbers, the real numbers or the integers, all have an order relation which satisfies these properties. But what is more important is what is missing. So, it is not true in a partially ordered set, it does not have to be true that any two elements are comparable.

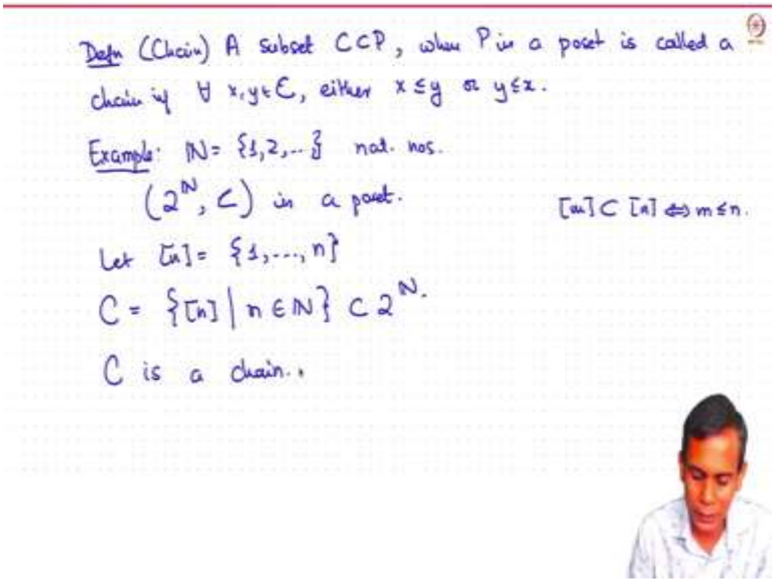
So, any two real numbers if you are given either they are equal, or one is less than the other, or the other way around. But in a partially ordered set, you could have pairs of elements for the x and y such that you neither have x less than or equal to y, nor do you have y less than or equal to x. So, this is weaker than the usual notion of order, which then in this context is called total ordering.

So, let us look at an example. Let us look at X any set and let 2 to the power x denote the power set of X. Then 2 to the power x the power set of X together with set containment, the relation of set containment is partial. Clearly, if a set x is contained in the set y; and a set y is contained in a set z, then the set x is contained in the set z. Then secondly, every set is contained in itself.

And thirdly, if a set x is contained in the set y and a set y is contained in the set x, then x and y are equal. So, the power set of any set forms a partially ordered set under containment. And note here that this is not a total order, because you can find two sets x and y such that neither x is contained in y nor is y contained in x provided of course, that the capital X the big universal set has at least two points.

And so now we have explained what is the meaning of partially ordered set. So, it is like an ordered set, but partial where not any two elements are comparable.

(Refer Slide Time: 08:14)



Defn (Chain) A subset $C \subset P$, where P is a poset is called a chain if $\forall\ x, y \in C$, either $x \leq y$ or $y \leq x$.

Example: $\mathbb{N} = \{1, 2, \ldots\}$ nat. nos.

$(2^{\mathbb{N}}, \subset)$ is a poset.

$[m] \subset [n] \Leftrightarrow m \leq n$.

Let $[n] = \{1, \ldots, n\}$

$C = \{[n] \mid n \in \mathbb{N}\} \subset 2^{\mathbb{N}}$.

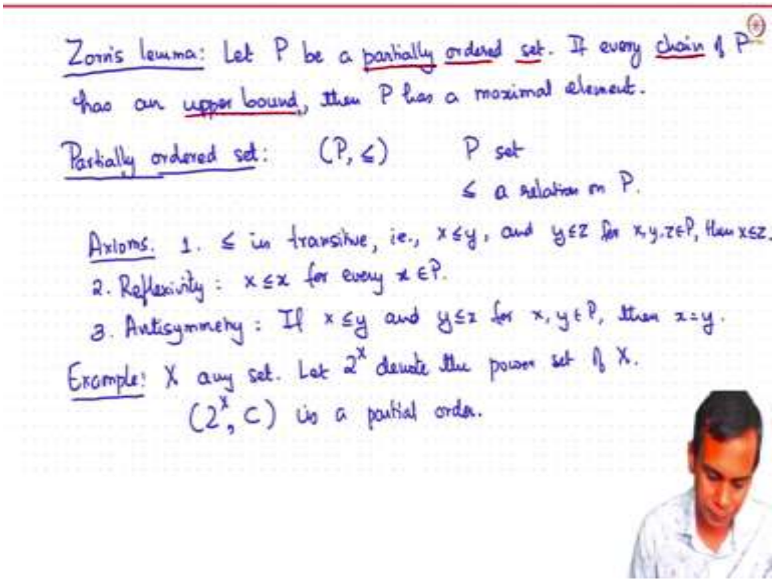
C is a chain..

Now next we come to the notion of a chain. So, let P be a partially ordered set. So, we define a chain, a subset C of P, where P is a partially ordered set. Now I will use this shorthand po set to denote partial, for partially ordered set. So, this p stands for partially, o stands for ordered, and set. So po set is just short for partially ordered set.

A subset of a po set is called a chain. If for all x and y in C, either x is less than or equal to y, or y is less than or equal to x. So, what we are saying is that when you take the partial order and restrict it to C, then you get a total order. Let us look at an example or a special case of the previous example. Consider N to be the set of natural numbers. And let us look at 2 to the power N under with with set inclusion.

So, this is a po set. And let box n denote the set as we have in algebra 1, the set of all integers between 1 and n. Then you look at C equals the collection box n, n belongs to N. This is a subset of 2 to the power N and C is a chain. Because any two elements of C will be of the form m and n and m is less or m is contained in n, is the same as saying that m is less than or equal to n. So, any two elements of C will be comparable. The ordering on the elements of C, will match with the ordering of the corresponding integers.

(Refer Slide Time: 12:49)



Zorn's lemma: Let P be a partially ordered set. If every chain of P has an upper bound, then P has a maximal element.

Partially ordered set: $(P, \leq)$ P set

$\leq$ a relation on P.

Axioms. 1. $\leq$ is transitive, ie., $x \leq y$, and $y \leq z$ for $x, y, z \in P$, then $x \leq z$.

2. Reflexivity : $x \leq x$ for every $x \in P$.

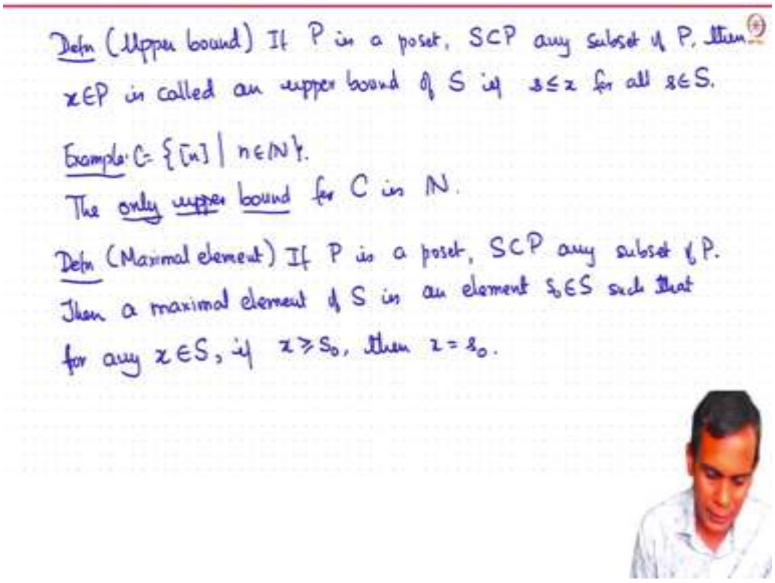
3. Antisymmetry : If $x \leq y$ and $y \leq x$ for $x, y \in P$, then $x = y$.

Example: X any set. Let 2^X denote the power set of X.

$(2^X, \subset)$ is a partial order.

So, we have also now defined chain and now, it remains to say well next I must tell you what does it mean for a chain to have an upper bound.

(Refer Slide Time: 10:54)

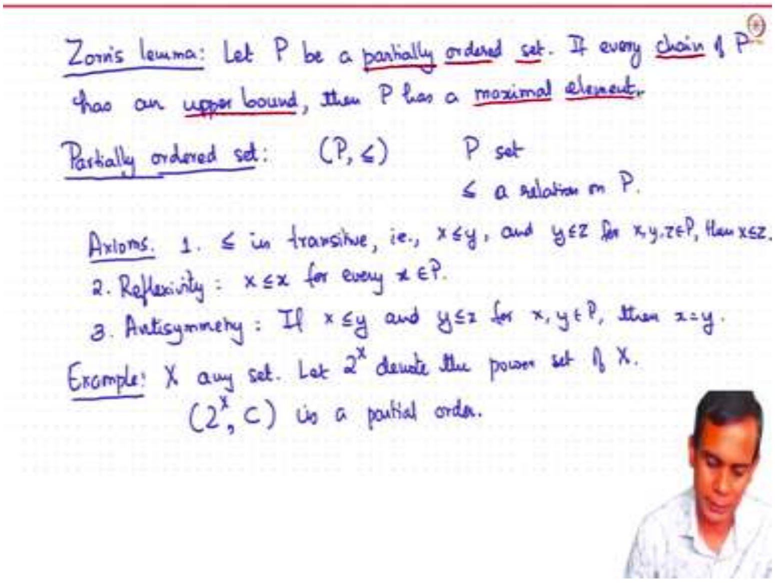


Defn (Upper bound) If P is a poset, $S \subset P$ any subset of P, then $x \in P$ is called an upper bound of S if $s \leq x$ for all $s \in S$.

Example: $C = \{[n] \mid n \in \mathbb{N}\}$.

The only upper bound for C is $\mathbb{N}$.

Defn (Maximal element) If P is a poset, $S \subset P$ any subset of P. Then a maximal element of S is an element $s_0 \in S$ such that for any $x \in S$, if $x \geqslant s_0$, then $x = s_0$.



Zorn's lemma: Let P be a partially ordered set. If every chain of P has an upper bound, then P has a maximal element.

Partially ordered set: $(P, \leq)$ P set

$\leq$ a relation on P.

Axioms. 1. $\leq$ is transitive, i.e., $x \leq y$, and $y \leq z$ for $x, y, z \in P$, then $x \leq z$.

2. Reflexivity: $x \leq x$ for every $x \in P$.

3. Antisymmetry: If $x \leq y$ and $y \leq x$ for $x, y \in P$, then $x = y$.

Example: X any set. Let 2^X denote the power set of X.

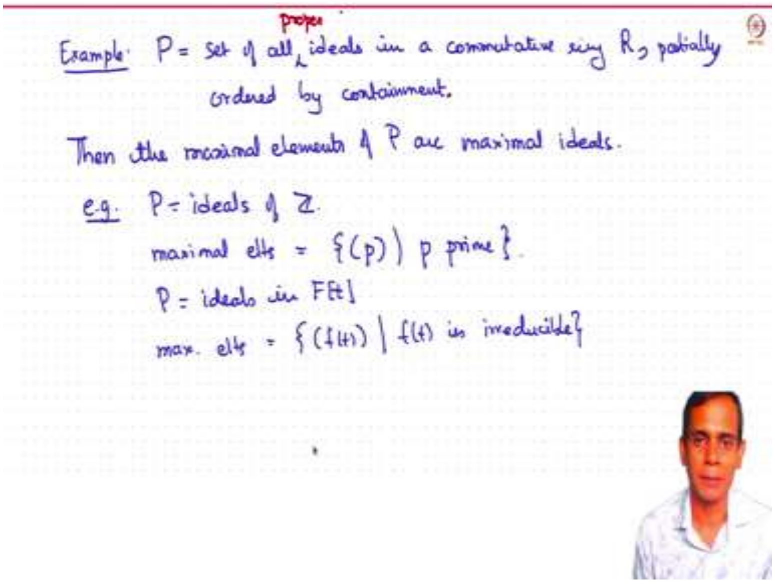
$(2^X, \subset)$ is a partial order.

So, let us go to the definition of an upper bound. If P is a partially ordered set and S is any subset of P, then an element x belongs to P is called an upper bound of S if, s is less than or equal to x, for all s in S. So, this element x is an upper bound for S means that it bounds every element of S. So, that explains upper bound.

In the example, if I take S to be, well what did we take last time, I called it C, the only upper bound for C is N itself. No other set contains all the subsets that are in the C. This is the only upper bound. So now we have also explained what is an upper bound. And this one last technical term here, which is that of a maximal element. So, what is the maximal element?

If P is a po set, S any subset, then a maximal element of S is an element S0 in S such that for any x in P, if x is greater than or equal to S0, or maybe I should say it like this for any x in S, if x is greater than S0, then x is equal to S0. So, there is no element of capital S, other than itself of capital, other than S0 which is greater than or equal to S0. So that is the definition of a maximal element. So, we have defined all the terms in this.

(Refer Slide Time: 14:40)



Example: P = set of all proper ideals in a commutative ring R, partially ordered by containment.

Then the maximal elements of P are maximal ideals.

e.g. P = ideals of $\mathbb{Z}$.

maximal elts = $\{(p) \mid p \text{ prime}\}$.

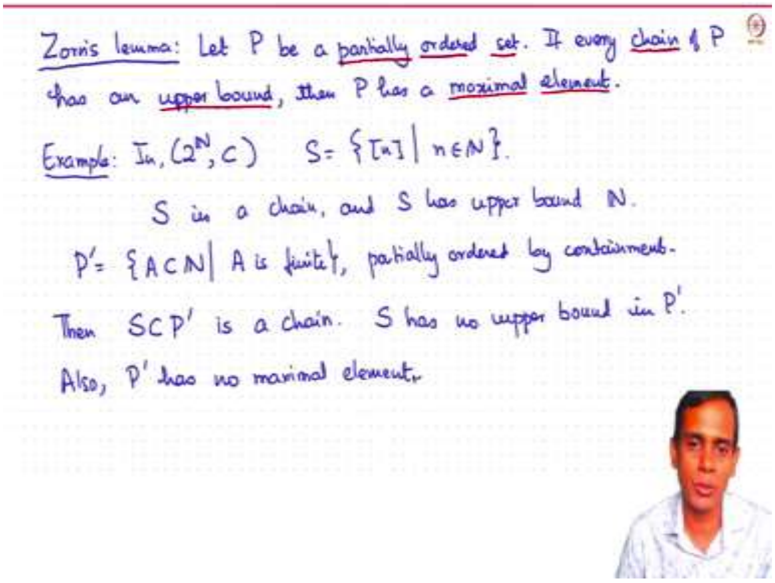
P = ideals in $F[t]$

max. elts = $\{(f(t)) \mid f(t) \text{ is irreducible}\}$

Let us just look at an example of maximal element. This you would be familiar with if you have done ring theory. So, let P be the po set of all, set of all ideals in a commutative ring R. Then a maximal element, and let us say we need to tell you what is the partial order, so partially ordered by containment. Actually, I do not want all ideals; I want all proper ideals, all proper ideals. Then the maximal elements of P are precisely what we call maximal ideals.

More specifically, if I take, if I take P to be ideals of Z, then then maximal elements are the ideals p generated by primes. And if I take P to be ideas in Ft where F is a field, then maximal elements are generated by ft, where ft is irreducible. This actually holds in any principal ideal domain. The maximal ideals of principal ideal domain are ideals generated by irreducible elements.

(Refer Slide Time: 16:54)



Zorn's lemma: Let P be a partially ordered set. If every chain of P has an upper bound, then P has a maximal element.

Example: In, $(2^{\mathbb{N}}, \subset)$ $S = \{[n] \mid n \in \mathbb{N}\}$.

S is a chain, and S has upper bound $\mathbb{N}$.

$P' = \{A \subset \mathbb{N} \mid A \text{ is finite}\}$, partially ordered by containment.

Then $S \subset P'$ is a chain. S has no upper bound in P'.

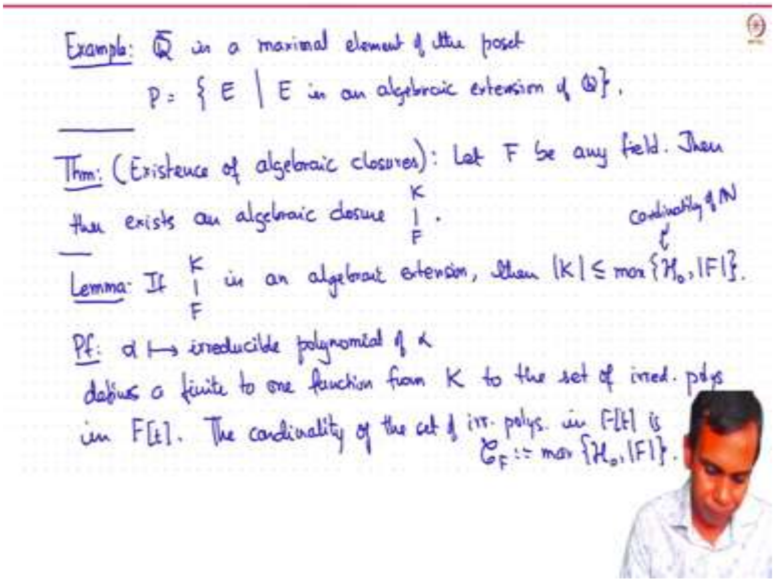
Also, P' has no maximal element.

So, now we know all the terms that appear in the statement of statement of Zorn's Lemma. If P is a partially ordered set, where every chain has an upper bound, then P has a maximal element. Let us look at an example where the hypothesis of Zorn's lemma does not hold and the conclusion does not either. So, take for example, P to be the set of power set of natural numbers under containment. And let us take S to N, where N is the natural number.

So, in this of course, this is a chain and S has upper bound N. But let us look at now P prime to be set of all finite subsets of N. So, let us look at all sets, A subset of N, such that A is finite, partially ordered by containment. Then S is still a subset of P, every set in NS is is finite. So S is a chain in P prime. But we saw that the only upper bound for S in P was the set of natural numbers itself. And so, S has no upper bound in P prime.

Also, there is no maximal element in P prime. P prime has no maximal element. Because if you were to take any finite subset of the natural numbers, you could always add one more element to it, one more natural number to it and get another finite subset of the natural numbers. So, P prime has no maximal elements.

(Refer Slide Time: 19:49)



Example: $\bar{\mathbb{Q}}$ is a maximal element of the poset

$P = \{ E \mid E \text{ is an algebraic extension of } \mathbb{Q} \}$.

Thm: (Existence of algebraic closures): Let F be any field. Then there exists an algebraic closure $\begin{matrix} K \\ | \\ F \end{matrix}$.

Lemma: If $\begin{matrix} K \\ | \\ F \end{matrix}$ is an algebraic extension, then $|K| \leq \max\{\underset{\text{cardinality of } \mathbb{N}}{\aleph_0}, |F|\}$.

Pf: $\alpha \mapsto$ irreducible polynomial of α defines a finite to one function from K to the set of irred. polys in F[t]. The cardinality of the set of irr. polys. in F[t] is $\mathcal{C}_F := \max\{\aleph_0, |F|\}$.

Now let us look at a good example of a maximal element. So, let us look at Q bar. So, Q bar is a maximal element of the po set P equals E over Q, where E is an algebraic extension. Let us just say E, where E is an algebraic extension. In fact, if you have any algebraic extension of Q, it is contained in Q bar, because E Q bar contains all the elements of the complex numbers which are algebraic over Q. And so, every algebraic extension is contained in Q bar. And therefore, Q bar is the maximal algebraic extension, it itself is algebraic of course.

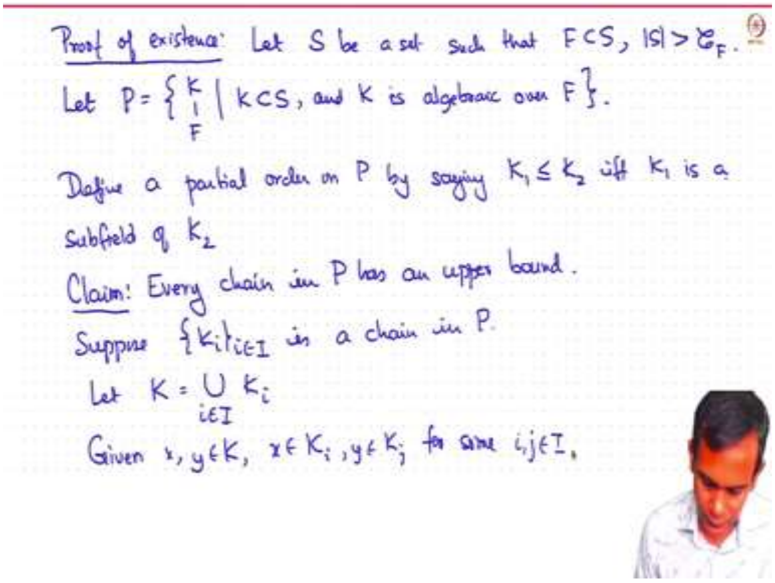
So, now, we can come to the statement of the theorem, which says that every field admits an algebraic closure. The theorem states that, so, this is the existence of algebraic closures, the main theorem of this lecture. Let F be any field, then F admits an algebraic closure there exists an algebraic closure K over F.

Now for the proof, before we jump into the proof, so, we will prove it by applying Zorn's lemma, we will construct certain partially ordered set of extensions and will show that all chains in that collection in that in that partially ordered set have upper bounds and then a maximal element of that partially ordered set, we will show it to be an algebraic closure of F.

But we need one slightly technical lemma for that. And the lemma is that if K over F is an algebraic extension, then the cardinality of K is less than or equal to the maximum of aleph 0 which is the cardinality of the natural numbers countable and the cardinality of F itself. We have seen this kind of argument when I explained to you that Q bar is a countable set.

So, basically, if you take an element alpha in K and send it to the irreducible polynomial of alpha, this defines a finite to one function from elements of K to the set of irreducible polynomials in Ft. And the cardinality of the set of irreducible polynomials in Ft, you can show quite easily is this number here; I will call it CF, maximum of aleph 0 and the cardinality of F. So, I will, I will not give you all the details of this, just think through it.

(Refer Slide Time: 24:56)



Proof of existence: Let S be a set such that $F \subset S$, $|S| > \mathscr{C}_F$.

Let $P = \left\{ \begin{matrix} K \\ | \\ F \end{matrix} \,\middle|\, K \subset S, \text{ and } K \text{ is algebraic over } F \right\}$.

Define a partial order on P by saying $K_1 \leq K_2$ iff K_1 is a subfield of K_2

Claim: Every chain in P has an upper bound.

Suppose $\{K_i\}_{i \in I}$ in a chain in P.

Let $K = \bigcup_{i \in I} K_i$

Given $x, y \in K$, $x \in K_i, y \in K_j$ for some $i, j \in I$.

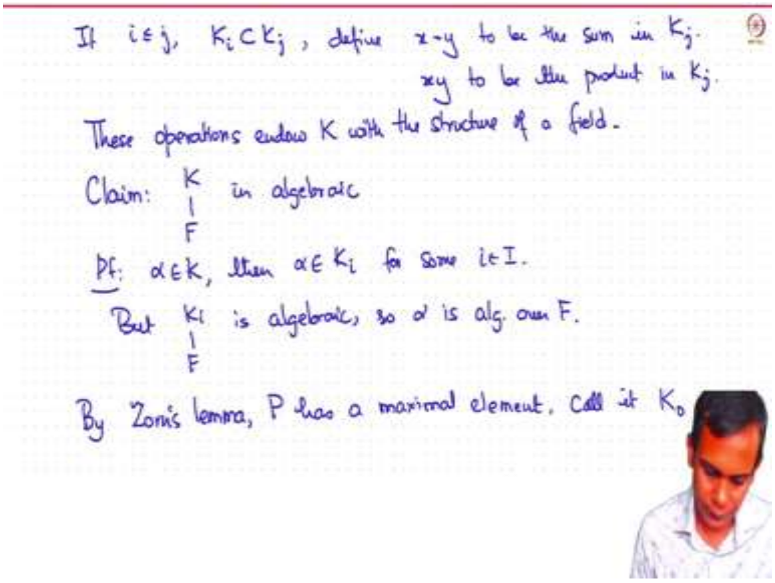
In any case, we will just use the statement. And now let us go on to the proof. So, proof of existence. So, to start with let S be a set with sufficiently large cardinality, such that firstly, F is contained in S; and secondly, cardinality of S is greater than CF. So, it is cardinality is strictly greater than the cardinality of any algebraic extension of F.

Now we will define the partially ordered set P. Let P be the set of all field extensions K over F, where K is realised as a subset of S, and K is algebraic over F. And define a partial order by saying that K1 is less than or equal to K2, if and only if K1 is a subset of K2. It is just the containment partial order.

And in particular, this would mean that K1 is a subfield of K2. So maybe I should be a little more careful because we talk about sets and sets with the structure of a field. So maybe I will see if K1 is a subfield of K2, or K2 is an extension of K1. Now, I claim that every chain in P has an upper bound. And the proof is the following.

So, suppose Ki i in I, is a chain in P. May not be accountable chain, any chain. Then let K be the union of all these sets. I will define a field structure on K. So, given x and y in K, we have x belongs to Ki, y belongs to Kj for some i j in I.

(Refer Slide Time: 27:56)



If $i \leq j$, $K_i \subset K_j$, define $x+y$ to be the sum in K_j.
xy to be the product in K_j.

These operations endow K with the structure of a field.

Claim: $\begin{array}{c} K \\ | \\ F \end{array}$ is algebraic

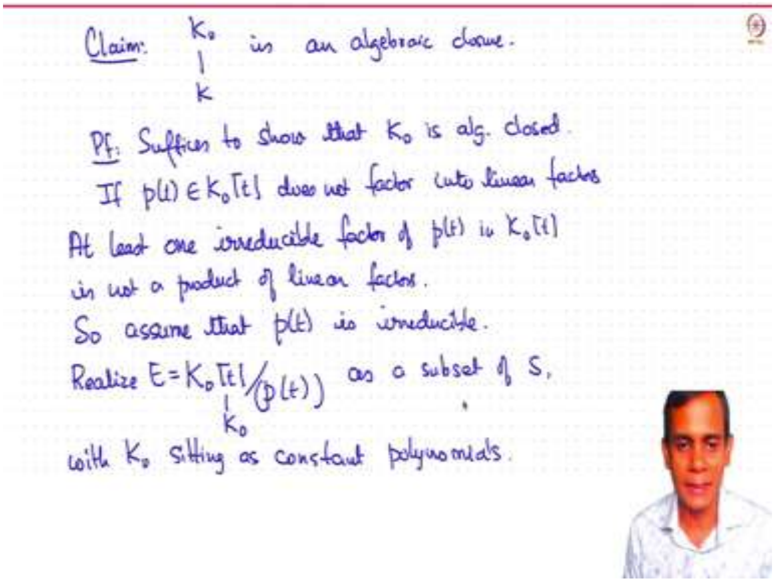
Pf: $\alpha \in K$, then $\alpha \in K_i$ for some $i \in I$.
But $\begin{array}{c} K_i \\ | \\ F \end{array}$ is algebraic, so α is alg. over F.

By Zorn's lemma, P has a maximal element. Call it K_0

Now, if i is less than or equal to j, then Ki is contained in Kj. And so, define x plus y to be the sum in Kj. And you can also define x plus x times y to be the sum in Kj. So, just define sum and product to be sums and products in the larger of the fields containing these elements. And then, because of the fact that our partial order insists that the subsets be sub fields, this will define give rise to a well-defined notion of sum and product in K and make K into a field. These operations endow K with the structure of a field.

Now, I need to show that K is algebraic over F. But this is easy because, if you take any alpha belonging to K, then alpha belongs to Ki for some i belongs to I and so, but Ki is algebraic over F, so, is algebraic. So, alpha is algebraic over F. And so, every chain in P has an upper bound, we have proved this. And so, the conclusion is by Zorn's lemma P has a maximal element. It would typically have more than one maximum element, but has at least one maximum element, call it choose one maximal element and call it K0.

(Refer Slide Time: 30:34)



Claim: $\begin{matrix} K_0 \\ | \\ K \end{matrix}$ is an algebraic closure.

Pf: Suffices to show that K_0 is alg. closed.

If $p(t) \in K_0[t]$ does not factor into linear factors

At least one irreducible factor of $p(t)$ in $K_0[t]$ is not a product of linear factors.

So assume that $p(t)$ is irreducible.

Realize $\begin{matrix} E = K_0[t]/(p(t)) \\ | \\ K_0 \end{matrix}$ as a subset of S,

with K_0 sitting as constant polynomials.

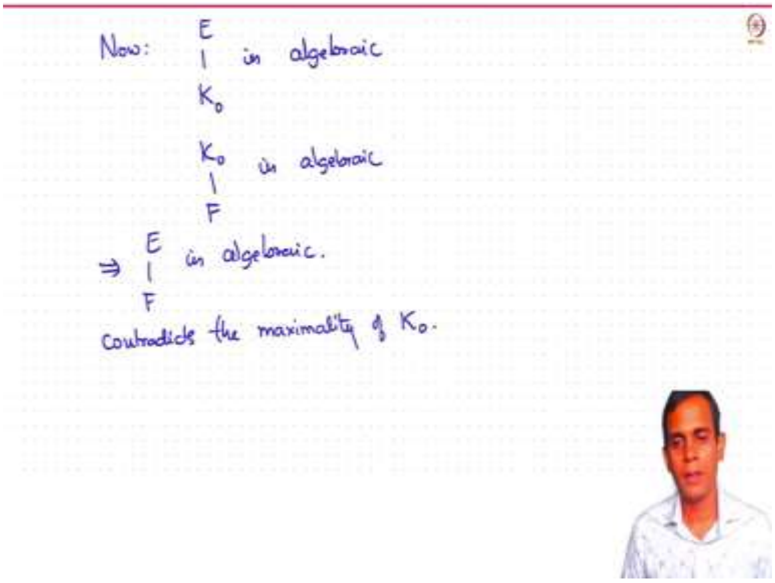
I claim that K0 over K is an algebraic closure. Since K0 over K is in t we know that K0 is algebraic over K. So, all I need to show is K0 is algebraically closed, suffices to show that K0 is algebraically closed. What we need to show is that every polynomial in K0 factors into linear factors. So, if Pt belongs to K0t does not factor into linear factors, we will try to get a contradiction.

Firstly, I want to reduce to the case where Pt is reducible. If Pt is not irreducible, then you factorise Pt into its irreducible factors. Each of those irreducible factors will not, at least one of those irreducible factors will not be a product of linear practice. So, at least one irreducible factor of Pt in K0t is not a product of linear factors, because, if each of these factors was a product of linear factors, then Pt itself would be a product of linear factors.

So, we can assume that Pt is irreducible, just replace Pt by its, one of its irreducible factors. Now, what you do is, realise the field extension K0t mod Pt as a subset. So, let us call this E. So, Pt is irreducible. So, Kt mod Pt is a field as a subset of S with K0 sitting as constant polynomials with sorry, yeah. So, we already have K0 is a subset of S. So, with K0 sitting as constant polynomials.

The reason we can do this is that S has a much larger, has a larger cardinality than K0 because the cardinality of K0 is this cardinality that we have written down here, the maximum of aleph 0 and the cardinality of S F. But S has cardinality strictly larger than that cardinality CF. So, then there is enough space inside S to take this polynomial ring and embed it inside S, in a way that puts K0 as constant polynomials.

(Refer Slide Time: 34:34)



Now: $\begin{array}{c} E \\ | \\ K_0 \end{array}$ is algebraic

$\begin{array}{c} K_0 \\ | \\ F \end{array}$ is algebraic

$\Rightarrow \begin{array}{c} E \\ | \\ F \end{array}$ is algebraic.

contradicts the maximality of K_0.

Then E is algebraic over K0 and K0 over F is algebraic, which implies that E over F is algebraic. This contradicts our assumption that K0 was maximal in P. So, the proof of the existence of the algebraic closure of any field is a fairly simple application of Zorn's lemma. Well, you have to be careful; we needed to fix the set S, so that we do not run into problems from set theory. But that is about it.