Galois' Theory Professor Dilip P. Patil Department of Mathematics Indian Institute of Science Bangalore Lecture No 58 Primitive Element Theorem

(Refer Slide Time: 00:25)



Ok so we have stated a Primitive Element theorem



(Refer Slide Time: 00:29)

for separable, finite separable extensions and we will prove it now. So the theorem we will prove is this is Primitive Element theorem. (Refer Slide Time: 00:53)



So let L over K be a finite field extension, finite separable field extension.

(Refer Slide Time: 01:11)

Theorem (Primitive element 1) Theorem) Let LIK bea finite separable field extension.

Then L over K is simple. This is what we want to prove.

(Refer Slide Time: 01:20)

Theorem (Primitive element 1) Theorem) Let LIK be a finite separable field extension. Then LIK is simple

Proof

Let me just mention

(Refer Slide Time: 01:25)

Theorem (Primitive element 1) Theorem) Let LIK be a finite separable field extension. Then LIK is simple Proof

that this was the most important step in Galois Theory. Galois was looking for primitive element for a separable extension.

His, in his time, all extensions considered were characteristic 0 fields. They were characteristic 0 fields therefore all were separable and they were all the time looking for primitive elements.

And that is very, very important step in the Galois Theory.

So, so let E over K be any algebraically closed field extension. Then what we have proved

(Refer Slide Time: 02:20)

Theorem (Primitive element 1) Let L/K be a finite separable field extension. Then L/K is primple Proof Let E/K be any algebraically closed field extra.

is then since L over K is separable, we know

(Refer Slide Time: 02:34)

Theorem (Primitive element () Theorem) Let L/K be a finite Separable field extension. Then L/K is simple Proof Let E/K be any algebraically closed field eath. Thun, since L/K is superable,

that if n is the degree of the field extension, this degree is also equal to the separable degree L over K S, and

(Refer Slide Time: 02:45)

Theorem (Primitive element Theorem) Let L/K be a finite Separable field extension. Then L/K is simple Proof Let E/K be any algebraically closed field extra. Then, since L/K is superable, M = [L:K] = [L:K]

separable degree is by definition, cardinality of the embeddings of L inside K, K embeddings of L inside K.

(Refer Slide Time: 02:53)

Theorem (Primitive element Theorem) Let L|K be a finite Separable field extension. Then L|K is primple Proof Let E|K be any algebraically closed field extra. Then, pinke L|K is separable, $M = [L:K] = [L:K] = \# Enb_K(L,E)$

So let us say that, that means these embeddings, there are precisely n embeddings. So let embedding set L E, this be exactly equal to $\sigma_1, \sigma_2, ..., \sigma_n$.

There are precisely n K embeddings

(Refer Slide Time: 03:17)

Theorem (Primitive element Theorem) Let L|K be a finite Separable field extension. Then L|K is primple Proof Let E|K be any algebraically closed field extra. Then, prime L|K is separable, $M = [L:K] = [L:K] = \# End_K(L,E)$ $Emb_{k}(L,E) = \{ \forall 1, \forall 2, \dots, \forall m \}$

of L into E. And what are we looking for? We are looking for an element z, so we are looking for an element $z \in L$

(Refer Slide Time: 03:43)



such that L equal to K(z).

Or equivalently this equality here will also follow from this inequality L over K bigger equal to K(z) over K

(Refer Slide Time: 04:18)



and this is equal to degree of $~~\mu_{z,K}~$,

(Refer Slide Time: 04:24)

We are looking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently 2 $[L:K] \ge [K(2):K] = deg/2, K$

this is n

(Refer Slide Time: 04:28)

We are looking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently $M = [L:K] \ge [K(2):K] = deg/2, K$

and this is bigger equal to, we have seen this degree is bigger equal to the zeroes, zeroes inside E but $\sigma_1(z), \dots, \sigma_n(z)$, they are all zeroes

(Refer Slide Time: 04:48)

We are looking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently $M = [L:K] \ge [K(2):K] = deg/2, K$

of mu, because the sigmas are K-algebra homomorphisms. And this, this number, (Refer Slide Time: 04:58)

We are looking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently $M = [L:K] \ge [K(2):K] = deg/M_{E,K}$ VI # { ~ (2) ... , ~ (2) }

so this number is also n because

(Refer Slide Time: 05:02)

We are looking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently $M = [L:K] \ge [K(2):K] = deg/M_{E,K}$ # { ~ (2) ... , ~ (2) }

these sigmas are uniquely determined by z

(Refer Slide Time: 05:07)

We are looking for an element $2 \in L$ Such that L = K(2) or equivalently 2 $M = [L:K] \ge [How]:K] = deg/M_{E}K$

on L.

So therefore this number will be n. So therefore all these inequalities will be equalities and we will get equality here and we will get

(Refer Slide Time: 05:19)

We are hooking for an element $2 \in L$ Such that L = K(2) or equivalently $M = [L:K] \ge \frac{\Gamma K(2):K}{2} = deg/2$

L equal to K(z).

So I want to check that, so in other words I want to find z, to find $z \in L$ such that

(Refer Slide Time: 05:39)

We are hooking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently 2 $M = [L:K] \ge [K(2):K] = deg/2, K$ V_1 $\# \{ \overline{\tau}_1(2), ..., \overline{\tau}_n(2) \}$ To find ZEL such that

the $\sigma_1(z),...,\sigma_n(z)$ are all distinct elements of E, they are elements of E, but the distinct is important.

(Refer Slide Time: 05:59)

We are hooking for an element
$$2 \in L$$

Such that $L \equiv K(2)$ or equivalently
 $M = [L:K] \ge [K(2):K] = deg/n_{\pm}K$
 $M = [L:K] = deg/n_{$

So once we achieve this then this number will be n and this μ , they are all zeroes of the minimal

(Refer Slide Time: 06:07)

We are hooking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently 2 $M = [L:K] \ge [K(2):K] = deg/2, K$ To find ZEL such that m $\overline{\tau_1(2)}, \cdots, \overline{\tau_n(2)}$ are all distributed E

polynomial, therefore the degree of the minimal polynomial will be bigger equal to this. Degree of the minimal polynomial

(Refer Slide Time: 06:12)

We are looking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently 2 $m = [L:K] \ge [K(2):K] = deg/m_{\Xi}K$ VI To find ze

is the degree of K(z) over K and z is contained in L therefore this degree is smaller

(Refer Slide Time: 06:18)

We are hooking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently $M = [L:K] \ge [K(2):K] = deg/2, K$ To find are all distinct ekmat of

equal to degree of L over K.

But this is precisely n. Therefore if I prove that these are distinct then all will be equalities here and this will follow,

(Refer Slide Time: 06:29)

We are looking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently $M = [L:K] \ge [K(2):K] = deg/M_{\Xi}, K$ M = [M] = M#{To find ZEL Such that m To find ZEL Such that m To find ZEL Such that m To find ZEL Such that m

clear.

Therefore our problem is to find z

(Refer Slide Time: 06:35)

We are hooking for an element $2 \in L$ Such that $L \equiv K(2)$ or equivalently 2 $M = [L: K] \ge [K(2): K] = deg/2, K$ $\forall I$ $\# \{ \tau (2) \dots \tau (2) \}$ To find 2 GL Such that m To find 2 GL Such that m To find 2 GL Such that m To find 2 GL Such that m

in L such that if I take, if I evaluate all embeddings of L into E at z the number should be different. Then all these elements should be different elements of E.

That is what we are looking for.

So this will imply L equal to K(z).

(Refer Slide Time: 06:56)

We are looking for an element $2 \in L$ Such that L = K(2) or equivalently 2 $M = [L: K] \ge [K(2): K] = deg/m_{z, K}$ L = K(z)

And we would finish our proof, Ok.

So how do we achieve that? I should have said in the beginning itself we may assume K is infinite.

Because if K

(Refer Slide Time: 07:10)



is finite and L over K is a finite field extension of a finite field then you already know that L cross is cyclic group.

And therefore L will be simple extension. So that is not a big deal.

So we are assuming

(Refer Slide Time: 07:27)



K is infinite field. And we will proceed the proof, so therefore L is a finite extension of K. So L will generated by x_1, \dots, x_r . (Refer Slide Time: 07:44)

Ne may assume K infinite L= K(x; ; , x+)

And by induction on r, induction on r, enough to prove that, enough to prove the case r equal to 2.

(Refer Slide Time: 08:02)

Ne may assume K infinite 3 L=K(x;;;, x) Induction on r. Etpt the case r=2

So that means what? We may assume L equal to, L is generated by 2 elements, now I will call them x and y.

(Refer Slide Time: 08:17)

We may assume K infinite 3 L=K(x;;, xr) Induction on r. Etpt the case r=2 We may assume L=K(x;y)

And I want to find an element z so that all values of different embeddings are different. So then, for any indices i and j, i not equal to j but in-between n and 1,

(Refer Slide Time: 08:42)

We may assume K infinite 3 L=K(x;;, x;) Induction on r. Etpt the case r=2 We may assume L=K(x;y) The for which is m Thun for 1 < i ≠ j ≤ m

these embeddings we know they are different.

(Refer Slide Time: 08:46)

We may assume K infinite 3 $L = K(x_i; ..., x_r)$ Induction on r. Etpt the case r=2We may assume $L = K(x_i; y)$ Thun for $1 \le i \ne j \le m$ $\sigma_i \ne \sigma_j$.

Therefore the values, these embeddings they are uniquely determined

(Refer Slide Time: 08:50)

We may assume K infinite 3 $L = K(x_i; ; x_r)$ Induction on r. Etpt the case r=2We may assume $L = K(x_i)$ Thun for $1 \le i \ne j \le m$ $\neq 5$:

by x and y, their values and x and y.

If I know $\sigma(x)$ and $\sigma(y)$ then that is uniquely determined because this L is generated by x and y.

So if I look at $(\sigma_i(x), \sigma_i(y))$, this pair, this is a pair of elements in E.

(Refer Slide Time: 09:13)

We may assume K infinite $L = K(x_{i}; ..., x_{p})$ Induction on r. Etpt the case r=2 We may assume $L = K(x_{j}y)$ Thun for $1 \le i \ne j \le n$ $\sigma_{i} \ne \sigma_{j}$ E 3 (5; (x), 5; (y))

And we have this $(\sigma_i(x), \sigma_i(y))$, this is also pair in E.

(Refer Slide Time: 09:23)

Ne may assume Kimfinite $L = K(x_{i}; ..., x_{r})$ Induction on r. Elept the case r=2We may assume $L = K(x_{j}y)$ Then for $1 \le i \ne j \le m$ $\sigma_{i} \ne \sigma_{j}$ $E \ni (\sigma_{i}(x), \sigma_{i}(y))$ $(\sigma_{j}(x), \sigma_{j}(y)) \in E$

So if they are different

(Refer Slide Time: 09:25)

We may assume K infinite $L = K(x_{i}; ..., x_{p})$ Induction on r. Etpt the case r=2 We may assume $L = K(x_{j}y)$ Thun for $1 \le i \ne j \le m$ $\sigma_{i} \ne \sigma_{j}$ $E \ni (\sigma_{i}(x), \sigma_{i}(y))$ $(\sigma_{i}(x), \sigma_{i}(y)) \in E$

these are different.

(Refer Slide Time: 09:27)

Ne may assume K infinite $L = K(x_{i}; ..., x_{i})$ Induction on r. Etpt the case r=2 We may assume $L = K(x_{j}y)$ Thun for $1 \le i \ne j \le m$ $\underline{\sigma} : \pm \underline{\sigma} :$ $E \ni (\overline{\sigma} : (x), \overline{\sigma} : (y)) \ne (\overline{\sigma} : (x), \overline{\sigma} : (y)) \in E$

Because if they are equal, each, each element of L

(Refer Slide Time: 09:32)

Ne may assume Kimfinite $L = K(x_{i}; ..., x_{r})$ Induction on r. Etpt the case r=2 We may assume $L = K(x_{i}y)$ Then for $1 \le i \ne j \le \frac{\sigma_{i}}{2} + \frac{\sigma_{i}}{2}$ $E \ni (\sigma_{i}(x), \sigma_{i}(y)) = (x_{i}, \sigma_{i}(y)) \in E$

is a combination

(Refer Slide Time: 09:33)

We may assume K infinite $L = K(x_{i}; .., x_{r})$ Induction on r. Etpt the case r=2 We may assume $L = K(x_{j}y)$ Then for $1 \le i \ne j \le m$ $\sigma_{i} \ne \sigma_{j}$ $E \ni (\sigma_{i}(x), \sigma_{i}(y)) \ne \sigma_{j}(y)) \in E$

of x and y and therefore these two numbers will be equal, so they will be So therefore for different i and j these pair of elements are different. So this is since, $(\sigma_i(x), \sigma_i(y))$, this pair uniquely determines σ_i , (Refer Slide Time: 10:08)

We may assume K infinite 3 $L = K(x_i, ..., x_r)$ Induction on r. Etypt the case r=2We may assume $L = K(x_iy)$ Thun for $1 \le i \ne j \le m$ $\underline{\sigma} : \pm \underline{\sigma} :$ $E \ni (\overline{\sigma} : (x), \overline{\sigma} : (y)) \ne (\overline{\sigma} : (x), \overline{\sigma} : (y)) \in E$ (fince $(\overline{\sigma} : (x), \overline{\sigma} : (y))$ wrightly determines $\overline{\sigma} :$

alright.

So now we have, to each embedding we have a pair. And now we consider a polynomial. So consider the polynomial

(Refer Slide Time: 10:30)



f T, this polynomial is product, product is running over pairs i comma j such that i is less than j. x is equal to n $(\sigma_i(x) + \sigma_i(y)T)$, this minus,

(Refer Slide Time: 11:00)

Consider the polynomial $f(T) = TT (\overline{\sigma}(x) + \overline{\sigma}(y)T)$ (Air. 15i<j<m

- $(\sigma_j(x) + \sigma_j(y)T)$.

(Refer Slide Time: 11:12)

Consider the polynomial (4) $f(T) = TT (\sigma(x) + \sigma(y)T)$ $I \le i \le j$ $-(\sigma(x) + \sigma(y)T)$

And then this is running over the product, this is like this.

(Refer Slide Time: 11:17)

Consider the polynomial (4) $f(T) = \prod \left[(\sigma_i(x) + \sigma_i(y)T) \right]$ $I \leq i < j \leq n - (\sigma_i(x) + \sigma_i(y)$ Air

So just stare at this polynomial.

Obviously this polynomial f is non zero first of all.

(Refer Slide Time: 11:27)



Because f 0 means what, at least one of the element in the product will be 0. But if the element in the product is 0, that means this $\sigma_i(x) + \sigma_i(y)T$ (Refer Slide Time: 11:40)

Consider the polynomial $f(T) = TT\left[(\sigma(x) + \sigma(y)T)\right]$ $I \le i < j \le m$ $f \ne 0$

will be equal to be, will be equal to $\sigma_i(x) + \sigma_i(y)T$

(Refer Slide Time: 11:44)



But as the polynomial in T, therefore $\sigma_i(x) = \sigma_j(x)$ and $\sigma_i(y) = \sigma_j(y)$ but i is different from j.

But that cannot happen. Because σ_i is different from σ_j .

Therefore f is non-zero.

Where are the coefficients of f? They are in E T.

(Refer Slide Time: 12:09)

Consider the polynomial (4) $f(T) = \prod \left[(\sigma \cdot (x) + \sigma \cdot (y)T) \right]$ $I \le i < j \le m - (\sigma \cdot (x) + \sigma \cdot (y)T)$ $f \neq 0, \quad f(T) \in E[T]$ (Air

Coefficients of f

(Refer Slide Time: 12:11)

Consider the polynomial $f(T) = TT \left[(\sigma \cdot (x) + \sigma \cdot (x)T) \right]$ $I \leq i < j \leq m$ $f \neq 0, \quad f(T) \in E[T]$

are this, they are elements, combinations of $\sigma_i \sigma(y)$ and $\sigma_j \sigma(y)$, all are elements of E therefore they are elements of T.

E is algebraically closed

(Refer Slide Time: 12:26)

Consider the polynomial (4) $f(T) = \prod \left[(\sigma \cdot (x) + \sigma \cdot (y)T) \\ 1 \le i < j \le m - (\sigma \cdot (x) + \sigma \cdot (y)T) \\ f \neq 0, \quad f(T) \in E[T] \\ \rightarrow alg.closed$

and we have a non-zero polynomial in algebraically closed field.

Therefore, therefore so in particular it has finitely many zeroes and all the zeroes are there.

V K, how many zeroes are in, now I look at the zeroes of this in K but this is contained in $V_E(f(T))$

(Refer Slide Time: 12:57)

and this is finite,

(Refer Slide Time: 13:00)

Consider the polynomial $f(T) = \prod \left[(\sigma_{i}(x) + \sigma_{i}(y)T) \\ i \leq i < j \leq m - (\sigma_{i}(x) + \sigma_{i}(y)T) \\ f \neq 0, \quad f(T) \in E[T] \\ \Rightarrow alg. closed \\ In particular, \quad \bigvee_{K} (f(T)) \leq \bigvee_{E} (f(T), \\ f(T)) \leq \sum_{K} (f(T)) \leq \sum_{K} (f(T), f(T)) \\ f(T) \in E[T] \\ f(T) \leq \sum_{K} (f(T)) \leq \sum_{K} (f(T), f(T)) \\ f(T) \in E[T] \\ f(T) \leq \sum_{K} (f(T)) \leq \sum_{K} (f(T), f(T)) \\ f(T) \leq \sum_{K} (f(T), f(T)) \\ f(T) \in E[T] \\ f(T) \leq \sum_{K} (f(T), f(T)) \\ f(T) = \sum_{K} (f(T), f(T)) \\$

therefore this is also finite. It may or may not have a 0,

(Refer Slide Time: 13:06)

Consider the polynomial $f(T) = \prod \left[(\sigma_{i}(x) + \sigma_{i}(y)) \right]$ $I \leq i < j \leq m - (\sigma_{i}(x) + \sigma_{i}(y))$ $f \neq 0, \quad f(T) \in E[T]$ $\Rightarrow alg.closed$ $In pariticular, \quad \bigvee (f(T)) \leq \bigvee (f(T))$ $f(T) \in f(T)$

but in any case it is a finite set. It may be empty set

(Refer Slide Time: 13:10)

Consider the polynomial $f(T) = \prod \left[(\sigma_{i}(x) + \sigma_{i}(y)T) \right]$ $I \leq i < j \leq m - (\sigma_{i}(x) + \sigma_{i}(y) + \sigma_{i}(y$

but it is finite,

(Refer Slide Time: 13:11)

Consider the polynomial

finite is important.

Now it is a finite set. So I can find an element which is outside that. So therefore there exists an element t in K such that f of t is non-zero (Refer Slide Time: 13:36)



because since K is infinite. Infinite field

(Refer Slide Time: 13:46)



and a polynomial is non-zero therefore it has zero, not all elements it is zero so at least element it is non-zero.

Now let z = x + yt. This is obviously an element in E,

(Refer Slide Time: 14:07)

Therefore $\exists t \in K$ such that $f(t) \neq 0$ (pince K so infinite) Let $z := x + yt \in E$ (Air

because

(Refer Slide Time: 14:09)

Therefore $\exists t \in K$ such that $f(t) \neq 0$ (Pince Krömfinite) Let $z := x + y t \in E$ Ai

t is in K, K is a subfield of E and x and y are in L and therefore they are, there is embedding so they are in elements of E also.

So these are the elements in, no what I am saying is actually they are elements in L

(Refer Slide Time: 14:30)

Thurefore I tek Such that (f(t) = 0 (Pince Krömfinite) Let Z:= x+yt E & L (Air

because x is in L, y is in L and t is in K therefore they are elements in L. Now I want to check that this z is

(Refer Slide Time: 14:38)



a required element.

So we may want to check, want to check that L equal to K(z). And that

(Refer Slide Time: 14:55)

Therefore $\exists t \in K$ such that 5 $f(t) \neq 0$ (pince Krömfinite) Let $z := x + yt \in E$ Namt to check that L = K[z]. (Air

will finish our proof, alright. So look at $\sigma_i(z)$ is, apply σ to this. Because sigma is a K-algebra homomorphism so this is $\sigma(x) + \sigma_i(yt)$

(Refer Slide Time: 15:14)

Thurefore $\exists t \in K$ such that 5 $f(t) \neq 0$ (Pince K so infinite) Let $z := x + yt \in E$ Namt to check that L = K[z]. $\sigma_i(z) = \sigma_i(x) + \sigma_i(yt)$ (Air,

but $\sigma_i(yt)$ is same as $\sigma_i(y)$ and

(Refer Slide Time: 15:21)

Therefore I tek Such that $f(t) \neq 0 \text{ (Pince Kromfinite)}$ Let $z_{:=} x + yt \in E$ Namt to check that L = K[z]. $\sigma_{i}(z) = \sigma_{i}(x) + \sigma_{i}(yt) = \sigma_{i}(x) + \sigma_{i}(y)$ (Air

 $\sigma_i(t)$ but σ is identity

(Refer Slide Time: 15:24)

Therefore I tek Such that 5 $f(t) \neq 0 \text{ (Pince Kromfinite)}$ Let $z_{:=} x + yt \in E L$ Namt to check that L = K[z]. $\sigma_{i}(z) = \sigma_{i}(x) + \sigma_{i}(yt) = \sigma_{i}(x) + \sigma_{i}(y)$ (Air.

on K, therefore this is just t.

(Refer Slide Time: 15:27)

Therefore I tek such that $f(t) \neq 0 \text{ (pine Kromfinit)}$ Let $z_{:=} x + yt \in \mathbf{E} L$ Namt to check that $L = K[\mathbf{z}]$. $\sigma_{i}(\mathbf{z}) = \sigma_{i}(\mathbf{x}) + \sigma_{i}(yt) = \sigma_{i}(\mathbf{x}) + \sigma_{i}(y)t$ (Air

Ok, on the other hand, Ok when I apply $\sigma_j(t)$, $\sigma_j(z)$, what do I get? I get this is $\sigma_j(x) + \sigma_j(yt)$.

(Refer Slide Time: 15:50)

Therefore I tek Such that $f(t) \neq 0 \text{ (Pince Kno infinit)}$ Let $Z := x + yt \in E$ L Namt to check that L = K[Z]. $\sigma_i(Z) = \sigma_i(x) + \sigma_i(yt) = \sigma_i(x) + \sigma_i(y)t$ (Air. $\sigma_{j}(z) = \sigma_{j}(x) + \sigma_{j}(y) t$

So i not equal to j.

Ok, but now note that i is, if i is different from j

(Refer Slide Time: 16:07)

Therefore $\exists t \in K$ such that 5 $f(t) \neq 0$ (pince K so infinite) Let $z := x + yt \in E$ L Namt to check that L = K[z]. $\sigma_i(z) = \sigma_i(x) + \sigma_i(yt) = \sigma_i(x) + \sigma_i(y)t$ $\sigma_j(z) = \sigma_j(x) + \sigma_j(y)t$ $(\neq j$

this cannot be equal to this. Both this cannot be equal to, so I claim that this is not equal,

(Refer Slide Time: 16:14)

Therefore $\exists t \in K$ such that 5 $f(t) \neq 0$ (Pince KND minit) Let $z := x + yt \in E$ L Namt to check that L = K[z]. $r_i(z) = r_i(x) + r_i(yt) = r_i(x) + r_i(y)t$ $f_j(z) = r_j(x) + r_j(y)t$ $(\neq j$

because if it is equal then, if it is equal here, if equality so I want to write the another color, if equality here, then what happens?

(Refer Slide Time: 16:31)

Therefore $\exists t \in K$ such that 5 $f(t) \neq 0$ (pince K so infinite) Let $z := x + yt \in E$ L Nome to check that L = K[z]. Nome to check that L = K[z]. $\overline{r}_i(z) = \overline{r}_i(x) + \overline{r}_i(yt) = \overline{r}_i(x) + \overline{r}_i(y)t$ $\overline{r}_j(z) = \overline{r}_j(x) + \overline{r}_j(y)t$ $(\neq j$

Then we get, we get this, this guy, $\sigma_i(x) + \sigma_i(y)T$ this $-\sigma_j(x) + \sigma_j(y)T$. This is one of the

(Refer Slide Time: 16:51)

Therefore $\exists t \in K$ such that 5 $f(t) \neq 0$ (pince K so infinite) Let $z := x + yt \in E$ L Namt to check that L = K[z]. $r_i(z) = \sigma_i(x) + \sigma_i(yt) = \sigma_i(x) + \sigma_i(y)t$ $f_j(z) = \sigma_j(x) + \sigma_j(y)t$ $(\neq j$ $(\tau_j(x) + \sigma_j(y)T) - (\sigma_j(x) + \sigma_j(y)T)$ T) - (+(x) + + (y)T)

factor in f. This is a factor in f. This factor will vanish at small t. That is the meaning of equality here.

So this equality means the factor of f, f(T) vanish, vanishes at t,

(Refer Slide Time: 17:20)

Therefore $\exists t \in K$ such that 5 $f(t) \neq 0$ (pine K so infinite) Let $2:=x+yt \in E$ L Namt to check that L = K[2]. Namt to check that L = K[2]. $f_i(2) = \sigma_i(x) + \sigma_i(yt) = \sigma_i(x) + \sigma_i(y)t$ $f_j(2) = \sigma_j(x) + \sigma_j(y)t$ $(\neq j)$ the factor $(\tau_i(x) + \sigma_i(y)T) - (\sigma_j(x) + \sigma_j(y)T))$ $f_i(T)$ vanishes at t

because equality here means when I evaluate it at T; that is equal here, so it is equal. But that will mean if a factor vanish then f of t will be 0.

(Refer Slide Time: 17:33)

Therefore $\exists t \in K$ such that 5 $f(t) \neq 0$ (pince K so infinite) Let $z_{:=} x + yt \in E$ L Namt to check that L = K[z]. Namt to check that L = K[z]. $\sigma_i(z) = \sigma_i(x) + \sigma_i(yt) = \sigma_i(x) + \sigma_i(y)t$ $f_j(z) = \sigma_j(x) + \sigma_j(y)t$ $(\dagger j)$ the factor $(\tau_i(x) + \sigma_i(y)T) - (\sigma_j(x) + \sigma_i(y)T)$ $\sigma_j(t) = \sigma_j(x) + \sigma_j(y) = \sigma_j(x) + \sigma_j(y)T$

But I have chosen f of t, so that

(Refer Slide Time: 17:37)

Therefore I tek Such that (Air f(t) = 0 (pine Krömfinite) Let z x+yt & A L = K[2]. that Want + (y+) = o: (x) + o: (y) t 5.(2) 01/2 - (- (x) + 5.(y) T the f f(t)=0

I have chosen t

(Refer Slide Time: 17:38)

Therefore I tek such that Air (pina Kró mfinite) f(七) = 0 AL 2:= X+ K[Z]. Want to che ·(x)+ ~: (y)t 5.(2) 5 (x) + ج(y) T f(t)=0

so that f of t is non-zero. So therefore this

(Refer Slide Time: 17:41)

Therefore $\exists t \in K$ such that $(f(t)) \neq 0$ (Rince K so infinite) Let $z_{:=} x + yt \in E$ L Namt to check that L = K[z]. Namt to check that L = K[z]. $\sigma_i(z) = \sigma_i(x) + \sigma_i(yt) = \sigma_i(x) + \sigma_i(y)t$ $\sigma_j(z) = \sigma_j(x) + \sigma_j(y)t$ (fj)the factor $(\tau_i(x) + \sigma_i(y)T) - (\sigma_j(x) + \sigma_j(y)T)$ $P_i(T)$ vanishes at t = f(t) = 0Ai of F(T) vanishes at t => f(t)=0

cannot be equal and therefore $\sigma_i(z)$ is not equal to $\sigma_i(z)$.

(Refer Slide Time: 17:47)

Thurefore $\exists t \in K$ such that $(f(t) \neq 0)$ (pince K so infinite) Let $z_{i} = x + yt \in E$ L Namt to check that L = K[z]. $\sigma_{i}(z) = \sigma_{i}(x) + \sigma_{i}(yt) = \sigma_{i}(x) + \sigma_{i}(y)t$ $f(z) = \sigma_{i}(x) + \sigma_{i}(y) + \sigma_{i}(y)t$ $f(z) = \sigma_{i}(x) + \sigma_{i}(y)t$ $f(z) = \sigma_{$

So I have done. That means I have chosen my z; so this means, this means, for this z $\sigma_1(z), \ldots, \sigma_n(z)$ are distinct elements of E and that is what we wanted

(Refer Slide Time: 18:26)

This means for this E: (b) $\tau_1(2), \tau_2(2), \cdots, \tau_n(2)$ are distinct elements of E.

to prove.

And this finish, this completes the proof.

(Refer Slide Time: 18:37)

This means for this E: $f_1(2), f_2(2), \dots, f_n(2)$ are distinct (find elements of E. This complete the proof.

Now I want to indicate also that, this proof we have done it by induction on the number of generators of L over K. L is a finite extension of K and by the induction on the number of generators of L over K we have proved that L over K is simple.

But one can also avoid the induction and directly prove it. So I just want to indicate that direct proof.

So another, so this is remark, this is remark,

(Refer Slide Time: 19:15)

This means for this E: $f_1(2), f_2(2), \dots, f_n(2)$ are distinct elements of E. This complete the proof. Kemark

one can do without induction as follows.

(Refer Slide Time: 19:30)

(in mo E: (i), 5(2), ..., 5, (2) are distinct elements of E. This completes the proof. Remark One can do without induction (i) follows:

So, so suppose L is a finite extension of K, therefore let us say L is generated by x_0, \ldots, x_n .

(Refer Slide Time: 19:47)

 $f_1(2), f_2(2), \dots, f_n(2)$ are distribut elements of E. This completes the proof. Remark One can do without induction so follows: Suppose $L = K(x_0, \dots, x_m)$ This means for this 2:

And now instead of, we can consider the following polynomial. Consider the polynomial

(Refer Slide Time: 20:02)

This means for this 2:

f, f T equal to product, 1 less equal to i less than j less equal to n and then the sum, sum is from k equal to 0 to m $\sigma_i(x_k)t^k$ minus summation k is from 0 to m $\sigma_j(x_k)T^k$.

(Refer Slide Time: 20:43)

This means for this 2:

And do the same, do the same trick. So instead of, do the same trick and use the fact that σ_i and σ_j , I will write in the next page, and use the fact that σ_i is uniquely determined by the tuple $\sigma_i(x_0), \ldots, \sigma_i(x_n)$.

(Refer Slide Time: 21:32)

and use the fact that Tris wrighely determined by the triple (J: (XD), ..., J; (Xm))

And same trick, so I will, so I would just say here, completed the proof, complete the proof. Is the same trick, no more extra trick is needed (Refer Slide Time: 21:52)

and use the fact that 5. is wrighed delemined by the tuple (5: (5), ..., 5; (5m)). Complete the proof.

for this, so that was what.

Now let us deduce some consequences from here.

So the first important consequence, so corollary,

(Refer Slide Time: 22:06)

ond use the fact that J. is wrighely determined by the tuple (J. (KD), ..., J. (Km)). Complete the proof. Corollay

let L over K be a finite separable extension

(Refer Slide Time: 22:24)

and use the fact that J. is uniquely delemined by the tuple (J. (XD), ..., J. (Xml)). Complete the proof. Corollary Let LIK bea finite Separable extension.

then f L over K, the set, this is the set of intermediary field extensions

(Refer Slide Time: 22:50)

and use the fact that J. is wrighed determined by the tuple (5: (x0), ..., 5; (xm)). Complete the proof. Corollary Let LIK bea finite Separable extension. Then F(4K) = the set of intermediany field extension

K contained in M contained in L,

(Refer Slide Time: 22:55)

and use the fact that J. is wrighely delemined by the tuple (J. (XD), ..., J. (Xm)). Complete the proof. Corollary Let LIK bea finite Separable extension. Then F(LK) = the set of intermediany field extension KEMEL.

this set, so this is the definition of that set.

Then this is a finite set. That means there are only finitely

(Refer Slide Time: 23:07)

and use the fact that J' is wrighed determined by the truple (J. (XD), ..., J. (Xm)). Complete the proof. Corollary Let LIK bea finite Suparable extension. Then F(L/K) (= the set of intermediany field extension K \le M \le L) No a fimite set.

many intermediary extensions.

So proof, proof, since L over K is finite separable, L over K is finite separable, we know it is simple. L is K[x] for some x by theorem.

(Refer Slide Time: 23:48)



And we want to check that this is a finite set. I want to check this is finite. So I am going to give you a map from this set to divisors of $D(\mu_{x,K})$. What is $D(\mu_{x,K})$?

(Refer Slide Time: 24:08)



This is, these are, this is the set of monic divisors of $\mu_{x,K}$ in the polynomial ring, in K[X].

(Refer Slide Time: 24:28)

Proof Since L/Kis finite separates T = K(x) for some $x \in L$ by Theorem $\exists (L|K) \longrightarrow D(M_x, K)$ H_{k} set of memic divisors of M_x, K in K[X]

This is a monic polynomial,

(Refer Slide Time: 24:29)

Proof Since L/Kis finite sepande L= K(x) for some x EL by Theore J(UK) ~ D(Mx II the set diviso KI

monic irreducible polynomial not in K[X] but in L[X].

(Refer Slide Time: 24:42)

Proof Since L/Kis finite separates L= K(x) for some x EL by Theorem J(LIK) ~>D(Mx,K) Hhe set of memic divisors of Mx, K Lot VI

It is a

(Refer Slide Time: 24:45)

Proof Since L/Kin finite spandle J(LIK) →D(Mx, H He set of divisors

a irreducible polynomial in K[X] but in

(Refer Slide Time: 24:49)

Proof Since L/Kis finite sepan L= K(x) for some x eL by The the set of m

L, when you go to L, it has a 0 in x so definitely this polynomial

(Refer Slide Time: 24:56)

Proof Since L/Kis finite separate L= K(x) for some x eL by The J(UK) ->D(Mx,K Hhe set q divisor

is not irreducible over L[X] so I look at the monic divisors of that polynomial in L[X]

And what is the map? Map is very simple. Take any M, intermediary field and look at the minimal polynomial of X over M.

This minimal polynomial of X over M and what is the relation between minimal polynomial of X over K, this divide this where in M[X] but if

(Refer Slide Time: 25:30)

Proof Since L/Kis finite separate L= K(x) for some x eL by Then = KII, = (LK) -> D(Mx,K) He set of momic divisors of Mx,K K[X] m Mark m M[X] > Mxm / M

it divides in M[X] then it will also divide in L[X] because L is bigger field. So our map is very simple, M going to the minimal polynomial of X over M. And I claim that this map is injective.

So the map we will check, we will prove, prove that this map, what is the map, M going to $\mu_{x,M}$ is injective.

What does that mean?

(Refer Slide Time: 26:09)



How does one prove that map is injective? That means if I know this

(Refer Slide Time: 26:13)

I We will prove that this map M → Mx, M is injective.

polynomial then I should get back this M.

So let us write this polynomial. Suppose this polynomial where, where, this is a monic polynomial of some degree. So suppose it is $X^m + a_{m-1}X^{m-1} + ... + a_1X + a_0$,

(Refer Slide Time: 26:38)

7 We will prove that this map $M \longrightarrow \bigwedge_{K,M} M$ injective. II M-1 $X + 0 X + \dots + 9 X + 90$

this is the polynomial in M[X].

(Refer Slide Time: 26:42)

7 We will prove that this map $M \longrightarrow \bigwedge_{x,M} M$ is injective. $X \stackrel{M}{\longrightarrow} \bigwedge_{x,M} X \stackrel{M-1}{\longrightarrow} X \stackrel{M-1}{\longleftarrow} X$

Then I say, then I want to prove M has to be equal to generated over K by these coefficients a_0, \dots, a_{m-1} .

(Refer Slide Time: 27:00)

I We will prove that this map $M \longrightarrow \bigwedge_{x, M} M$ is injective. $X \xrightarrow{m} g X \xrightarrow{+\cdots} + g X + g$ $K \xrightarrow{+} g \longrightarrow X \xrightarrow{+\cdots} + g X + g$ $K \xrightarrow{+} g \longrightarrow X \xrightarrow{+\cdots} + g \xrightarrow{+} + + g \xrightarrow{+} + g$

If I prove this then injectivity

(Refer Slide Time: 27:03)

I We will prove that this map $M \longrightarrow \bigwedge_{K \in M} M$ is injective. II m-1 $\chi^{m} = \chi^{m} \chi^{+\dots+q} \chi^{+q_{0}}$ $\in M[X]$ Then $M = K(q_{0}, \dots, q_{m-1})$

will follow because if I know the polynomial, I can get that my field M. So I have to prove this equality. But to prove this equality, let us call this as M_0

(Refer Slide Time: 27:16)



and obviously this is contained here because this polynomial

(Refer Slide Time: 27:19)

I We will prove that this map $M \longrightarrow \bigwedge_{x, M} M$ is injective. $M \longrightarrow \bigwedge_{x \neq 0} M^{-1}$ $X + \binom{m-1}{2} \times (a_0, \dots, q_{m-1}) =: M$ Thun $M \ge K(a_0, \dots, q_{m-1}) =: M$

has coefficients in M.

So this is ob/obvious, so this is clear. So I have to prove the other way.

So to prove the other way I just have to compute this, this, everything is a subfield of L.

So I want to compute L over M and also I want to compute L over M_0 .

And I want to show they are equal.

(Refer Slide Time: 27:46)

I We will prove that this me $M \longrightarrow \bigwedge_{x, M} M$ is injective. $X^{m} \stackrel{H}{} \stackrel{M-1}{X + \dots + q} \stackrel{X+q_{0}}{X + q_{0}}$ $\in M[X]$ Then $M \stackrel{M}{\cong} \kappa(q_{0}, \dots, q_{m-1}) =: M_{0}$ From [L:M] [L:M]

If I show they are equal then M will be equal to M_0 because this is a subfield, therefore this, this equal to L over M over, now times M over M_0 , this I know.

(Refer Slide Time: 28:04)

7 We will prove that this me [L:M] [L:M. L:M)M:M

So if I prove that this equal to this, then M over M_0

(Refer Slide Time: 28:08)

I We will prove that this map $M \longrightarrow \bigwedge_{x, M} M$ is injective. $X^{m} \stackrel{M}{\to} X^{m-1} \xrightarrow{X^{m-1}} M_{X} \xrightarrow{X^{m-1}} M_{X}$ = M [X]Then $M \stackrel{2}{\to} K(a_{0}, \dots, g_{m-1}) =: M_{0}$ [L:M] L:M Mi

is 1, and M will be equal to M_0 .

So I am aiming to prove these are equal.

But, Ok what is this? This is L is generated by x over K therefore M is also generated by x over M.

(Refer Slide Time: 28:25)

The will prove that this map
$$9$$

 $M \longrightarrow M_{X,M}$
 $i i i j e dive. \qquad II \qquad m-1 \\ X &= 0 \qquad X + \cdots + q \\ X + q \qquad X + \cdots + q \\ X + \qquad$

Therefore this equal, degree of this, this is a simple extension over M. So this is the degree of

 $\mu_{x,M}$.

(Refer Slide Time: 28:38)



But $\mu_{x,M}$, this is same thing as degree of μ_{x,M_0} because

(Refer Slide Time: 28:49)

7 We will prove that this map $M \longrightarrow \bigwedge_{x, M} M$ is injective. $\chi_{+ q}^{m} q \chi_{+ \dots + q}^{m-1} \chi_{+ q_{0}} \chi_{+ q_{0}}$ $\in M[X]$ Then $M \ge \kappa(a_{0}, \dots, q_{m-1}) =: M_{0}$ L: M] = deg/mxm = deg/mxma ME×] [L:m][M:M]

these two polynomials are same, because the coefficients are same.

Therefore these two polynomials are same. These polynomials individually, they are same. This polynomial and this polynomial are equal therefore their degrees are equal.

(Refer Slide Time: 29:02)

I We will prove that this m $M \longrightarrow \bigwedge_{x, M} M$ is injective. $X^{m} \stackrel{M}{\to} X^{+\dots+q} \stackrel{X+q_{0}}{X+q_{0}} \stackrel{X+\dots+q}{\to} \stackrel{X+q_{0}}{\to} \stackrel{X+\dots+q}{\to} \stackrel{X+\dots+q}{\to} \stackrel{X+q_{0}}{\to} \stackrel{X+\dots+q}{\to} \stackrel{X+q_{0}}{\to} \stackrel{X+\dots+q}{\to} \stackrel{X+\dots+q}$ MEX

And by the same argument this equality,

(Refer Slide Time: 29:07)

The will prove that this map
$$9$$

 $M \longrightarrow M_{x,M}$
 $M \longrightarrow M_{x,M}$

therefore these are equal. Therefore from here you conclude M equal to M_0 and therefore

(Refer Slide Time: 29:15) We will prove that this " $\frac{dive}{X + q} = \frac{11}{X + q} \frac{m-1}{X + q} \frac{\chi}{\chi + q_0}$ $\in M[X]$ $M \ge K(q_0, \dots, q_{m-1}) =: M_0$ injective. N Then

we conclude the map is injective.

The map is injective.

So if you want to give the name δ , the map δ is injective.

(Refer Slide Time: 29:33)

We will prove that the 9 X+..+9 X+90 K(ao,..., 9m-1)=: M Then MZ MEX

So that proves that, so if you have a injective map from some set to a set where the bigger set is finite, this is a finite set

(Refer Slide Time: 29:44)

f Since L/Kin finite separate = K(x) for some x EL by Them 10 1.7 M

because this is a monic polynomial of some degree and therefore the number of divisors, monic divisors will be also finitely many.

Therefore

(Refer Slide Time: 29:55)

Vemil $X \stackrel{m}{+} \underset{(m-1)}{X + \cdots + q} X + q_{0}$ $\in M[X]$ $\in M[X]$ $K(q_{0}, \cdots, q_{m-1}) =: M_{q}$ M Ihen

we finish the proof and next time we will continue therefore the consequences of this very important theorem,



and we will also use this to compute some examples of some Galois groups. So thank you and we will continue next time.