Math 491, Tuesday, March 31 Chapter 21 Fields

Wed- Exam 19/20 8:30

Thu- 21

Fri - 21

Sun 11:59 PM Project Proposal

Mon- Problem Session, Sage 21

$F(\alpha) \cong F[x]/\langle p(x) \rangle$ ← min poly Im $\phi_\alpha = F(\alpha)$?

Linear Algebra

E extension of $F \Rightarrow E$ vector space w/ F as scalars

vectors, set E addition: $\alpha, \beta \in E$ $\alpha + \beta = \alpha + \beta$ (define ↑, field ↑)

scalar multiplication: $\alpha \in F$, $\beta \in E$

define → $\alpha\beta = \alpha\beta$ ← field E

Theorem $E = F(\alpha)$, α algebraic over F of degree n $\Rightarrow$ $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ basis of E as a vector space over F.

Proof $\beta \in E$ then $\beta \in F(\alpha) \cong \frac{F[X]}{\langle p(x) \rangle}$ $= \underline{\mathrm{Im}(\phi_\alpha)}$

$\phi_\alpha : F[X] \to E$, $\phi_\alpha(p(x)) = p(\alpha)$, with q as q

$\beta = q(\alpha)$ for some poly $q \in F[X]$

$= a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m$ $a_i \in F$

linear combination of vectors $1, \alpha, \alpha^2, \ldots, \alpha^m$ with scalars $a_0, a_1, \ldots, a_m$

Divide $q(x)$ by $p(x)$, min poly of α

$q(x) = s(x)\,p(x) + r(x)$ degree $r(x) < n$

$\beta = q(\alpha) = s(\alpha)\,p(\alpha) + r(\alpha) = s(\alpha)\cdot 0 + r(\alpha) = r(\alpha)$

$= b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ So S spans E.

Suppose $c_0 1 + c_1\alpha^1 + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = \underset{\sim}{0} = 0_E$ RLD

If some $c_i \neq 0$ then $t(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1}x^{n-1}$

w/ ① $t(\alpha) = 0$ ② degree $t <$ degree of p ③ $t(x) \neq 0$

$\Rightarrow\Leftarrow$ minimality of $p(x)$ So $c_0 = c_1 = \cdots = c_{n-1} = 0 \Rightarrow$ S linearly independent

Defn E/F (E extension of F). Suppose E/F is a finite dimensional vector space, then E is a finite extension of degree n & we write $[E:F] = n$

"degree" of poly of alg element = finite extension

Theorem If E is a finite extension of F, then E is an algebraic extension of F.

Proof Set $[E:F] = n$ (degree of extension)

Grab $\beta \in E$ (show β is an algebraic element)

$T = \{1, \beta, \beta^2, \beta^3, \ldots, \beta^{n-1}, \beta^n\} \subseteq E$ $n+1$ vectors from n-dimensional vector space

So T linearly dependent. there are scalars $d_0, d_1, \ldots, d_n$, not all zero w/ $\in F$

$$d_0 1 + d_1 \beta + d_2 \beta^2 + \cdots + d_{n-1}\beta^{n-1} + d_n \beta^n = \underline{0} = 0_E$$

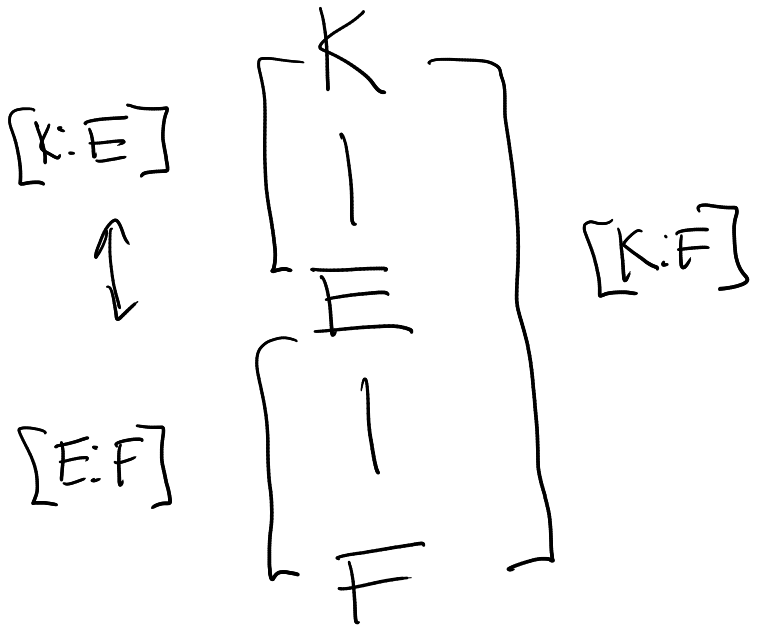
Set $s(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_{n-1}x^{n-1} + d_n x^n \in F[x]$

So $s(\beta) = 0$, so β is a root of a polynomial in $F[x]$

$\Rightarrow$ β algebraic over F.

Theorem E/F finite extension, K/E finite extension $\Rightarrow K/F$ finite extension

plus $\underline{[K:F]} = \underline{[K:E][E:F]}$



Like "Lagrange's theorem"