Theorem Let $E = F(\alpha)$ ← Simple extension, $\alpha \in E$ algebraic over F

Suppose degree of α over F is n. Then every element $\beta \in E$ can be expressed uniquely in the form

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

for $b_i \in F$

Proof:

$\phi_\alpha(F[x]) \supseteq F(\alpha)$ $\therefore$ every $\beta \in E = F(\alpha)$

is

$$\beta = \phi_\alpha(f(x)) = f(\alpha)$$ ← Poly in α with coefficients in F.

Let

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$ be the min. poly of α

$$p(\alpha) = 0 \quad \therefore \quad \alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$$

Now note

$$\alpha^{n+1} = \alpha\,\alpha^n = -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha$$

$$= a_{n-1}(-a_{n-1}\alpha^{n-1} - \cdots - a_0) - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha$$

By induction α^m, $m \geq n$ can be written as linear combinations of powers of α less than n

$\therefore \beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$

Now show above expression is unique

If $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$

$g(x) = (b_0 - c_0) + (b_1 - c_1)x + \cdots + (b_{n-1} - c_{n-1})x^{n-1} \in F[x]$

and $g(\alpha) = 0$ but $\deg(g) < \deg(p)$

$\therefore g(x) = 0 \quad \therefore \quad b_i = c_i \quad \forall i$ ∎

Ex] $E = \mathbb{R}[x]/\langle x^2+1\rangle$ ← field extension of $\mathbb{R}$ ($\mathbb{R}(i)$)

contains a root $\alpha = x + \langle x^2+1\rangle$ (From a proof before)

$\alpha^2 = x^2 + \langle x^2+1\rangle$

$= -1 + \langle x^2+1\rangle$

$\therefore \alpha^2 = -1$ in E

$\phi : \mathbb{R}(\alpha) \to \mathbb{C}$ is an isomorphism

$a + b\alpha \mapsto a + bi$

Note: Last theorem Lets us think of $E = F(\alpha)$ as a vector space with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$

Def] If E is an extension field of F which is a finite dim. v.space over F of dim $= n$ we say E is a finite extension of degree n over F

write $[E:F] = n$

Theorem Every finite extension field E of F is an algebraic extension.

Proof:

Let $\alpha \in E$, $[E:F] = n$

then $1, \alpha, \ldots, \alpha^n$ can not be linearly ind.

$\therefore$ $\exists\ a_i \in F$, not all zero, s.t.

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0$$

$\therefore$ $p(x) = a_n x^n + \cdots + a_0 \in F[x]$

$\neq 0$

and $p(\alpha) = 0$ $\therefore$ E is an alg. extension.

∎

Thm If E is a finite extension of F and K is a finite extension of E then K is a finite extension of F and

$$[K:F] = [K:E][E:F] \qquad F \subset E \subset K.$$

Proof: Let $\{\alpha_1, \ldots, \alpha_n\}$ ($n = [E:F]$) be a basis for E as an F-vector space and $\{\beta_1, \ldots, \beta_m\}$ ($m = [K:E]$) be a basis for K as a E-vectorspace

Show $\{\alpha_i \beta_j\}$ forms a basis for K over F.

Show spans. Let $u \in K$ arbitrary, then

$$u = \sum_{j=1}^{m} b_j \beta_j \quad \text{and} \quad b_j \in E$$

Since $b_j \in E \Rightarrow b_j = \sum_{i=1}^{n} a_{ij} \alpha_i \quad a_{ij} \in F$

$$\therefore \quad u = \sum_{j=1}^{m} \sum_{i=1}^{n} \underbrace{a_{ij}}_{\in F} \beta_j \alpha_i$$

$\therefore \{\alpha_i \beta_j\}$ spans K over F.

Show $\{\alpha_i \beta_j\}$ are lin. ind

$$u = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} \alpha_i \beta_j = 0 \in K \quad , c_{ij} \in F$$

$$= \sum_{j=1}^{m} \underbrace{\left(\sum_{i=1}^{n} c_{ij} \alpha_i \right)}_{\in E} \underbrace{\beta_j}_{\beta_j\text{'s are lin independent over } E} = 0$$

$$\sum_{i=1}^{n} c_{ij} \alpha_i = 0 \quad \forall j$$

α_i are lin. ind. over F

$\Rightarrow c_{ij} = 0. \quad \forall ij$

$\{\alpha_i \beta_j\}$ is a basis ∎

cor If F_i is a field, $i = 1, \dots, k$ $\quad F_k \supset \cdots \supset F_1$

and if F_{i+1} is a finite extension of F_i then

- F_k is a finite extension of F_1

and

$$[F_k : F_1] = [F_k : F_{k-1}] \cdots [F_2 : F_1].$$

cor Let E be an exten. of F. If $\alpha \in E$ is alg. over F with minimal poly. $p(x)$ and $\beta \in F(\alpha)$ with min. poly $q(x)$ then

$$\deg(q(x)) \mid \deg(p(x))$$

Proof:

$$\deg(p(x)) = [F(\alpha) : F]$$

$$\deg(q(x)) = [F(\alpha) : F(\beta)]$$

$$F \subset F(\beta) \subset F(\alpha) \subset E$$

$$[F(\alpha) : F] = [F(\alpha) : F(\beta)] \cdot [F(\beta) : F]$$

$= \deg(p(x))$ $\qquad$ $= \deg(q(x))$

■

Ex Determine $\mathbb{Q}(\sqrt{3} + \sqrt{5})$

The min poly. of $\sqrt{3} + \sqrt{5}$ is

$$x^4 - 16x^2 + 4$$

$$[\mathbb{Q}(\sqrt{3}+\sqrt{5}):\mathbb{Q}] = 4$$

- $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$

$\therefore \sqrt{3}+\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$

$\{1, \sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$ and

$\{1, \sqrt{5}\}$ is a basis for $(\mathbb{Q}(\sqrt{3}))(\sqrt{5})$ over $\mathbb{Q}(\sqrt{3})$

$\therefore$ $\updownarrow$ $\quad\quad$ $=\mathbb{Q}(\sqrt{3},\sqrt{5})$

$\{1, \sqrt{3}, \sqrt{5}, \sqrt{3}\cdot\sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{3},\sqrt{5})$

over $\mathbb{Q}$ and

$$\dim(\mathbb{Q}(\sqrt{3},\sqrt{5})) = 4$$

$$\sqrt{3}+\sqrt{5} \in \mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3}+\sqrt{5})$$

$\therefore$ a simple extension of degree 4

can have $F(\alpha_1, \ldots, \alpha_n) = F(\alpha)$.

$$F(\alpha) \cong F[x]/\langle p(x)\rangle$$

poly degree $< n$

Theorem 21.22. *Let E be a field extension of F. Then the following statements are equivalent.*

1. *E is a finite extension of F.*
2. *There exists a finite number of algebraic elements $\alpha_1, \ldots, \alpha_n \in E$ such that $E = F(\alpha_1, \ldots, \alpha_n)$.*
3. *There exists a sequence of fields*

$$E = F(\alpha_1, \ldots, \alpha_n) \supset F(\alpha_1, \ldots, \alpha_{n-1}) \supset \cdots \supset F(\alpha_1) \supset F,$$

where each field $F(\alpha_1, \ldots, \alpha_i)$ is algebraic over $F(\alpha_1, \ldots, \alpha_{i-1})$.

Proof: See Book

Thm Let E be a field extension of F. The set of elements in E that are alg. over F form a field.

Proof: Let α, β be alg. over F

$\Rightarrow$ $F(\alpha, \beta)$ is a finite extension and all elements of $F(\alpha, \beta)$ are alg. over F

$\therefore$ $\alpha \pm \beta$, $\alpha\beta$, α/β $(\beta \neq 0)$ are alg. over F

$\therefore$ $F(\alpha, \beta)$ is a field. ∎

Cor The set of all algebraic numbers (complex num. alg. over $\mathbb{Q}$) is a field

Def Let E be a field extension of F.

$\overline{F}$, the algebraic closure of F in E is the field consisting of all $\alpha \in E$ s.t. α is alg. over F.

- F is algebraically closed $(F = \overline{F})$ if every non-constant polynomial in $F[x]$ has a root in F.

Thm A field F is algebraically closed iff every non-constant poly. factors into linear factors over $F[x]$.

Proof (sketch):

$\forall\ p(x) \in F[x]$ $\quad \deg(p(x)) = n$ have a zero in F, let α be that zero

$\therefore \quad p(x) = (x-\alpha)\, q_1(x)$ $\quad \deg(q_1(x)) = \deg(p) - 1$

Now apply to $q_1(x)$

and so on... gives a linear factorization

Conversly if we have a linear factorization ....

then $ax-b$ will apear and gives a root $\frac{b}{a}$

Cor An algebraically closed field F has no proper algebraic extension E ∎