$F(\alpha)/F$, if $\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^n$ are linearly indp,

then $\deg m_\alpha > n$.

So if $\alpha = \sqrt{2} + \sqrt{3}$, $F = \mathbb{Q}$,

then $m_\alpha(x) = x^4 - 10x^2 + 1$

(in fact, in this case, it's enough to check that $\alpha^0, \alpha^1, \alpha^2$ are lin. indp. since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ and $\deg m_\alpha \mid$ some field containing α. ... (Find out why))

$[K : F] < \infty$, $\alpha \in K$. Consider $\varphi : K \to K$, $\varphi(\beta) = \alpha\beta$.

$\varphi \in \mathrm{End}_F K$ since $\varphi(a\beta) = a\varphi(\beta)$, $\varphi(\beta_1 + \beta_2) = \varphi(\beta_1) + \varphi(\beta_2)$.

claim: $m_\varphi = m_\alpha$.

if $f \in F[x]$, then $f(\varphi)$ is multiplication by $f(\alpha)$.

$\varphi^2(\beta) = \alpha^2\beta$, ...

$f(\varphi) = 0 \iff f(\alpha) \cdot \beta = 0 \quad \forall \beta \iff f(\alpha) = 0$.

So ideals $\underset{\mathrm{Ann}(\varphi)}{\underset{\shortparallel}{\{f : f(\varphi) = 0\}}} = \{f : f(\alpha) = 0\} = (m_\alpha) = (m_\varphi)$.

<u>Example</u>: $\alpha = \sqrt{2} + \sqrt{3}$

$$\alpha \cdot 1 = \sqrt{2} + \sqrt{3}$$

$$\alpha \cdot \sqrt{2} = 2 + \sqrt{6}$$

$$\alpha \cdot \sqrt{3} = 3 + \sqrt{6}$$

$$\alpha \cdot \sqrt{6} = 3\sqrt{2} + 2\sqrt{3}$$

So matrix of φ is $\begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$

<u>Claim</u> Invariant factors of φ are all equal to m_α, and $C_\varphi = m_\alpha^{n/d}$ where $n = [K:F]$, $d = \deg_F \alpha$.
$= [F(\alpha):F]$.

And $K = F(\alpha)$ iff $C_\varphi = m_\alpha$.

Let $\{\overset{1}{\overset{\shortparallel}{\beta_1}}, \dots, \beta_\ell\}$ be a basis of K over $F(\alpha)$.

$(\ell = n/d)$

Then $K = F(\alpha) \oplus F(\alpha)\cdot\beta_2 + \cdots + F(\alpha)\cdot\beta_\ell$.

$$\beta_i \longleftrightarrow 1$$

$\forall i$, $F(\alpha)\cdot\beta_i \cong F(\alpha)$ as $F[x]$-modules (with $x \cdot \eta = \alpha\eta$).

isomorphic $F[x]$-modules,

Matrix: 

Matrix: $\begin{pmatrix} \square & & \\ & \ddots & \\ & & \square \end{pmatrix}$ isomorphic $F[x]$-modules, companion matrices of m_α.

$\alpha \in K$, $F(\alpha)/F$ - simple extension

Case 2: α is transcendental over F: $\nexists \overset{\neq 0}{f} \in F[x]$ s.t. $f(\alpha) = 0$

Then
$$\begin{aligned} F[x] &\longrightarrow K \\ x &\longmapsto \alpha \\ f(x) &\longmapsto f(\alpha). \end{aligned}$$
has 0 kernel

$F[\alpha]$ is not a field.

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in F[x],\ g \neq 0 \right\}$$

We have a hom'sm $F(x) \longrightarrow K$,
$$F(x) = \left\{ \frac{f(x)}{g(x)} : f, g \in F[x],\ g \neq 0 \right\}$$

with 0 kernel, so $F(x) \cong F(\alpha)$.

"α behaves like a variable"

eg $\quad \mathbb{Q}(\pi) \cong \mathbb{Q}(x)$

$$\underline{f(\pi)} \longleftrightarrow \underline{f(x)}$$

$\overline{g(\pi)}$ $\overline{g(x)}$

α is algebraic $\iff$ $[F(\alpha) : F] < \infty$.

Otherwise, $F(\alpha) \cong F(x)$, and $[F(x) : F] = \infty$.

Let $K = F(\alpha_1, \dots, \alpha_n)$ – K/F is finitely generated.

Then we have a tower

$$\begin{array}{c} K_n = F(\alpha_1,\dots,\alpha_n) \\ | \\ K_{n-1} = F(\alpha_1,\dots,\alpha_{n-1}) \\ \vdots \\ | \\ K_1 = F(\alpha_1) \\ | \\ K_0 = F \end{array}$$

$\forall i$, $K_i = K_{i-1}(\alpha_i)$.

So this is a tower of simple extensions.

If $\deg_F \alpha_i < \infty$ (α_i is algebraic over F),

Then $\deg_{K_{i-1}} \alpha_i < \infty$ (α_i is algebraic over K_{i-1})

$$\begin{array}{c} \deg_{K_{i-1}} \alpha_i \\ \wedge\!\!| \\ \deg_F \alpha_i \end{array}$$

Then $[K:F] = [K=K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot \cdots \cdot [K_1 : K_0 = F]$

$$= \deg_{K_{n-1}} \alpha_n \cdot \cdots \cdot \deg_F \alpha_1$$

$$\leq \deg_F \alpha_1 \cdot \cdots \cdot \deg_F \alpha_n$$

So any finitely generated extension K/F is a tower of simple extensions

It's finite iff all the generators are algebraic over F. $\quad ([K:F] \geq [F(\alpha_i):F])$

And, in this case, $[K:F] \leq \prod$ degrees of generators.

K/F extension, $\alpha_1, \ldots, \alpha_n \in K$.

Then $F[\alpha_1, \ldots, \alpha_n]$ is the ring / also F-algebra generated by $\alpha_1, \ldots, \alpha_n$.

$F(\alpha_1, \ldots, \alpha_n)$ is the field " "

Theorem: If $\alpha_1, \ldots, \alpha_n$ are algebraic over F, then

$$F(\alpha_1, \ldots, \alpha_n) = F[\alpha_1, \ldots, \alpha_n].$$

Proof induction, use the tower.

Assume that K/F is an extension, L_1/F, L_2/F are finite sub-extensions.

$L_1 L_2$ - composite of L_1 & L_2

$$\begin{tikzcd}
 & L_1L_2 \arrow[dl, dash, "\leq n_2"'] \arrow[dr, dash, "\leq n_1"] \arrow[dd, dash, "m"] & \\
L_1 \arrow[dr, dash, "n_1"'] & & L_2 \arrow[dl, dash, "n_2"] \\
 & F &
\end{tikzcd}$$

$n_1 \mid m$, $n_2 \mid m$.