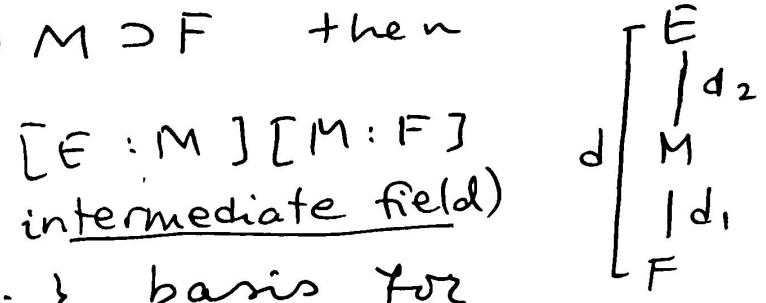
MATH 403/503 - L33

Th If $E \supset M \supset F$ then

$$[E:F] = [E:M][M:F]$$

(M is called an intermediate field)



Pf Let $\{\alpha_i\}$ basis for M over F and $\{\beta_j\}$ basis for E over M. We claim $\{\alpha_i\beta_j\}$ is a basis for E over F.

Spans: Let $e \in E$. Since $\{\beta_j\}$ spans E over M,

$$e = \sum_j \mu_j \beta_j$$

for some $\mu_j \in M$. Since $\{\alpha_i\}$ spans M over F,

$$\mu_j = \sum_i \varphi_{ji} \alpha_i$$

for some $\varphi_{ji} \in F$. So

$$e = \sum_j \mu_j \beta_j = \sum_j \left(\sum_i \varphi_{ji} \alpha_i\right) \beta_j =$$

$$= \sum_{j,i} \varphi_{ji} \alpha_i \beta_j$$

So $\{\alpha_i\beta_j\}$ spans E over F.

Lin Indep. Suppose

$$\sum_{i,j} \phi_{ij}\, \alpha_i \beta_j = 0$$

for some $\phi_{ij} \in F$. Then

$$\sum_j \left(\sum_i \phi_{ij}\, \alpha_i \right) \beta_j = 0$$

Since $\{\beta_j\}$ lin indep over M and $\sum_i \phi_{ij} \alpha_i \in M$ for each j, we have

$$\sum_i \phi_{ij} \alpha_i = 0 \qquad \forall j$$

Since $\{\alpha_i\}$ lin indep over F,

$$\phi_{ij} = 0 \qquad \forall i \; \forall j.$$

Thus $\{\alpha_i \beta_j\}$ lin indep over F. ∎

Cor. If $F_1 \subset F_2 \subset \cdots \subset F_m$ then

$$[F_m : F_1] = [F_m : F_{m-1}] \cdots [F_3 : F_2][F_2 : F_1]$$

Cor. If E/F is a field extension and $\alpha \in E$ is algebraic over F and $\beta \in F(\alpha)$, then

$$\deg m_\beta(x) \mid \deg m_\alpha(x)$$

where $m_\alpha = m_{\alpha,F}$ and $m_\beta = m_{\beta,F}$ are the minimal polynomials over F.

Pf. $F \subset F(\beta) \subset F(\alpha) \subset E$ and

$$[F(\alpha) : F] = \deg m_{\alpha,F}(x) =: d_\alpha$$

$$[F(\beta) : F] = \deg m_{\beta,F}(x) =: d_\beta$$

By the Degree Formula,

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

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

so $d_\beta \mid d_\alpha$. ∎

Th. Every finite extension is algebraic.

Pf. Let E/F be finite (i.e. $[E:F] < \infty$) and let $\alpha \in E$. Then

$$\{1, \alpha, \alpha^2, \dots\} \subset E$$

Cannot be linearly independent so $\sum_{i=0}^{n} c_i \alpha^i$ for some $c_i \in F, n > 0$ and not all $c_i = 0$. WLOG $c_n \neq 0$, then WLOG $c_n = 1$

Let $p(x) = \sum_{i=0}^{n} c_i x^i$ (Note: $p(x) \neq 0$)

Then $p(\alpha) = 0$ so α is algebraic over F.

Since every $\alpha \in E$ is algebraic over F, E/F is algebraic.

∎

Ex.

1) $\alpha = \sqrt[5]{3+\sqrt{2}}$ Show α is alg/$\mathbb{Q}$.

Sol: $\alpha^5 = 3+\sqrt{2}$

$\alpha^5 - 3 = \sqrt{2}$

$(\alpha^5 - 3)^2 = 2$

$\alpha^{10} - 6\alpha^5 + 7 = 0$

$0 \neq p(x) = x^{10} - 6x^5 + 7 \in \mathbb{Q}[x]$, $p(\alpha) = 0$

2) $\beta = \sqrt{3}+\sqrt{5}$. Find basis for $\mathbb{Q}(\beta)/\mathbb{Q}$.

Sol: $\beta^2 = 3 + 2\sqrt{15} + 5 \Rightarrow \left(\frac{\beta^2 - 8}{2}\right)^2 = 15$

$\Rightarrow \beta^4 - 16\beta^2 + 64 = 60 \Rightarrow \beta^4 - 16\beta^2 + 4 = 0$

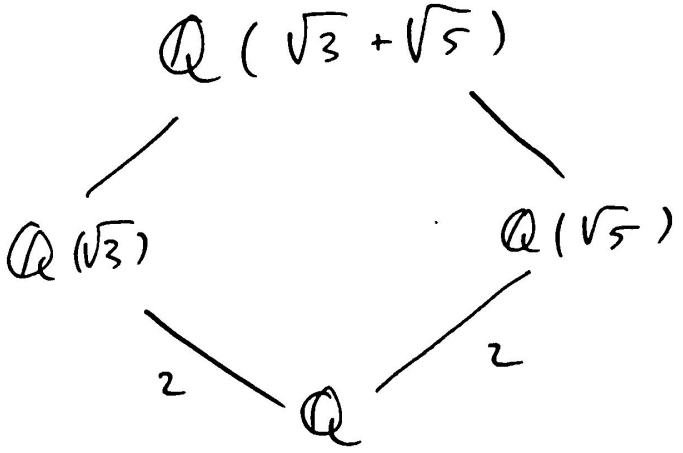
Let $p(x) = x^4 - 16x^2 + 4$

If we could show $p(x)$ was irreducible/$\mathbb{Q}$ then $\{1, \beta, \beta^2, \beta^3\}$ is a basis for $\mathbb{Q}(\beta)/\mathbb{Q}$.

Instead we consider

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}+\sqrt{5})$$
$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subseteq \uparrow$$

$\left(\frac{1}{\sqrt{3}+\sqrt{5}} = \frac{\sqrt{3}-\sqrt{5}}{3-5}\right.$ shows $\left.\sqrt{3}, \sqrt{5} \in \mathbb{Q}(\sqrt{3}+\sqrt{5})\right)$



We write the degree of the extension between the fields in the Hasse diagram.

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

So $\sqrt{5} = a + b\sqrt{3}$

$5 = a^2 + 3b^2 + 2ab\sqrt{3} \Rightarrow \sqrt{3} \in \mathbb{Q}$ contrad.

So $[\mathbb{Q}(\sqrt{3}+\sqrt{5}) : \mathbb{Q}(\sqrt{3})] \geq 2$

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

$=$

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

$2 \leq d \leq 2$ $\qquad$ 2

$\Rightarrow d = 2$