Proposition: Let F be a field with extension field E. Let $\alpha \in E$ be algebraic over F. If $\deg(\alpha, F) = n$,

$\deg(\alpha, F) = \deg(\mathrm{irr}(\alpha, F))$

Then every $\beta \in F(\alpha)$ is algebraic over F, and $\deg(\beta, F) \le \underbrace{\deg(\alpha, F)}_{n}$.

Pf: Consider $\{\underbrace{1, \beta, \beta^2, \ldots, \beta^n}_{n+1 \text{ elements of } F(\alpha)}\}$ must be a linearly dependent set over F $\Rightarrow \exists\, c_0, c_1, \ldots, c_n \in F$ s.t.

$$p(\beta) = c_0 + c_1\beta + c_2\beta^2 + \cdots + c_n\beta^n = 0 \quad \text{ie}$$

β is algebraic over F, and $\mathrm{irr}(\beta, F)$ is a factor of this polynomial — so $\deg(\beta, F) \le n$. ☐

An algebraic extension of a field F is an extension field E of F s.t. every $\beta \in E$ is algebraic over F.

[Example if α is alg. over F, $F(\alpha)$ is alg. extension by the Prop. above.]

Even more $F(\alpha, \beta, \gamma) = ((F(\alpha))(\beta))(\gamma)$ is also an alg. extension of F.]

A finite extension E of a field F is one such that

$[E : F]$ = degree of E/F = (dim of E as a vector space over F)

is finite.

Thm An extension field E of a field F is a finite extension $\Longleftrightarrow$ E is an algebraic extension that is finite.

[Every finite extension field is algebraic.]

Proof: Let $\alpha \in E$. Suppose $[E:F]=n$.

Then $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ is lin. dependent

$\Rightarrow \exists$ constants $c_0, c_1, \dots, c_n \in F$ s.t.

$$c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$$

$\Rightarrow \alpha$ is alg. over F. ☒

Tower Theorem: If K, L, M are fields such that $K \leq L \leq M$, then

$$[M:K] = [M:L][L:K].$$

(Cor. $F_1 \leq F_2 \leq \dots \leq F_r \Rightarrow [F_r:F_1] = [F_r:F_{r-1}] \cdot \dots \cdot [F_2:F_1]$ by induction)

Proof: Let $\{u_1, \dots, u_a\}$ be a basis for L/K, where $a=[L:K]$

Let $\{v_1, \dots, v_b\}$ be a basis for M/L, where $b=[M:L]$.

Consider the set $B = \{u_i v_j : 1 \leq i \leq a, 1 \leq j \leq b\} \subseteq M$

Note $|B| = ab$.

First, we show B spans M over K

$\forall w \in M$, $\exists$ elements $c_1, \dots, c_b \in L$ s.t.

$$w = c_1 v_1 + c_2 v_2 + \cdots + c_b v_b = \sum_{j=1}^{b} c_j v_j.$$

Since $c_j \in L$, $\exists$ elements $d_{j,1}, \dots, d_{j,a} \in K$ s.t.*:

$$c_j = \sum_{s=1}^{a} d_{j,s} u_s, \text{ for each } j.$$

Thus $w = \sum_{j=1}^{b} \sum_{s=1}^{a} (d_{j,s}) u_s v_j$.

$\therefore$ B spans M over K. ✓

Next. we show B is linearly indep over K.

Suppose $\sum_{j=1}^{b} \underbrace{\left(\sum_{s=1}^{a} (d_{j,s}) u_s \right)}_{\in L} v_j = 0$ for some $d_{j,s} \in K$.

Since $\{v_j\}$ is lin. indep over L, $\forall j$,

$$\left(\sum_{s=1}^{a} \underbrace{d_{j,s}}_{\in K} u_s \right) = 0 .$$

Since $\{u_s\}$ is lin. indep over K,

then $d_{j,s} = 0 \ \forall s, \forall j$.

$\therefore$ B is a lin. indep set over K.

$\therefore$ B is a basis for M.

$\Rightarrow$ M has dim $ab = [M:K]$ over K.

$\therefore$ $[M:K] = [M:L][L:K]$. $\blacksquare$

$\therefore$ We can strengthen our proposition above.

If α is alg over F, $\beta \in F(\alpha)$, then

$$\deg(\beta, F) \mid \deg(\alpha, F).$$

Examples

① In the homework, we showed

$[\mathbb{Q}(\sqrt{2}+i\sqrt{5}):\mathbb{Q}]=4$

Notice $\mathbb{Q}(\sqrt{2}+i\sqrt{5}) \subseteq (\mathbb{Q}(\sqrt{2}))(i\sqrt{5})$ ☆

$\mathbb{Q}(\sqrt{2})$ has deg 2

$(\mathrm{irr}(\sqrt{2},\mathbb{Q}) = x^2-2)$

$i\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$

But it satisfies $x^2+5 = \mathrm{irr}(i\sqrt{5}, \mathbb{Q}(\sqrt{2}))$.

$\therefore [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$

$[(\mathbb{Q}(\sqrt{2}))(i\sqrt{5}):\mathbb{Q}(\sqrt{2})] = 2$

$\therefore [\mathbb{Q}(\sqrt{2}, i\sqrt{5}):\mathbb{Q}] = 2\cdot 2$ by Tower Theorem.

In the homework: $[\mathbb{Q}(\sqrt{2}+i\sqrt{5}):\mathbb{Q}]=4$

by ☆ $\mathbb{Q}(\sqrt{2}+i\sqrt{5}) = (\mathbb{Q}(\sqrt{2}))(i\sqrt{5})$.

---

② Consider $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

$\sqrt{2}$ has degree 2 over $\mathbb{Q}$.

$\sqrt[3]{2}$ has degree 3 over $\mathbb{Q}$

$\therefore \sqrt{2}$ has degree 2 over $\mathbb{Q}(\sqrt[3]{2})$. ← basis $1, 2^{1/3}, 2^{2/3}$

x^2-2 ← basis $1, 2^{1/2}$

$[\mathbb{Q}(\sqrt[3]{2},\sqrt{2}):\mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[3]{2},\sqrt{2}):\mathbb{Q}(\sqrt[3]{2})]}_{2}\underbrace{[\mathbb{Q}(2^{1/3}):\mathbb{Q}]}_{3} = 6$

$\therefore \mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$ has basis $\{1, 2^{1/3}, 2^{2/3}, 2^{1/2}, 2^{5/6}, 2^{7/6}\}$

Notice $2^{7/6} = 2 \cdot 2^{1/6}$, so $2^{1/6} \in \mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$

$= \mathbb{Q}(2^{1/6})$. simple extension!!