Combining Prop 2.9, Thm 2.5, Thm 2.4 we get

Thm 2.11 Let $K:F$ be a field extention $\alpha \in K$ algebraic over F. Then

1) $F[\alpha] = F(\alpha) \cong F[x] / (m_{\alpha,F}(x))$

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

3) $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis of $F(\alpha)$ as a F-vector space.

Thm 2.11 says that if α is alg/F then $[F(\alpha):F] < \infty$

In fact we have

Prop 2.12 An element α is algebraic over F if and only if $[F(\alpha):F] < \infty$.

Proof ($\Rightarrow$) Thm 2.11 (2)

($\Leftarrow$) Conversly suppose $[F(\alpha):F] = n < \infty$. Since $F(\alpha)/F$ has dimension n then the $n+1$ elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ of $F(\alpha)$ must be lin. dependent.

Hence $\exists$ $b_0, b_1, \ldots b_n \in F$, not all zero such that

$b_0 + b_1\alpha + \dots + b_n\alpha^n = 0$.

Hence α is a root of $b_0 + b_1x + \dots + b_nx^n \in F[x]$ and is algebraic over F $\blacksquare$.

Cor 2.13 If $K:F$ is a finite extension then K is algebraic over F

Proof: Let $\alpha \in K$ any elt of K. Then w.t.s α is algebraic over F

We have that $F \subset F(\alpha) \subset K$ and

$$[K:F] = [K:F(\alpha)][F(\alpha):F].$$

Since by assumption $[K:F] < \infty$ we have in particular that $[F(\alpha):F] < \infty$. Then by Prop 2.12

α is alg. over F. Since $\alpha \in K$ was arbitrary $K:F$ is algebraic

$\blacksquare$

Rmk: Converse is False

ie K/F alg $\not\Rightarrow [K:F] < \infty$.

Eg. $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$.

Then $\overline{\mathbb{Q}}$ is a field, $\overline{\mathbb{Q}} : \mathbb{Q}$ algeb. of infinite degree (Exercise serie 3)

There is however a 'partial converse'

First we give/recall some definitions

Defn ① An extension $K : F$ is called finitely generated if $\exists$ elements $\alpha_1, \ldots, \alpha_n \in K$ s.t. $K = F(\alpha_1, \ldots, \alpha_n)$ = smallest subfield of K containing F and $\alpha_1, \ldots, \alpha_n$.

② If K_1, K_2 are 2 subfields of K. The composite field of K_1 and K_2 is the smallest subfield of K containing K_1 and K_2. It is denoted by $K_1 K_2$

If $F \subset K_1, K_2 \subset K$ then
$K_1 K_2 = F(K_1 \cup K_2)$

Rmk. $F(\alpha, \beta) = F(\alpha)(\beta)$ by minimality of fields in question

Thm 2.14 An extension $K : F$ is finite if and only if K is generated over F by a finite number of algebraic elements $\alpha_1, \ldots \alpha_n$ over F.
ie $K = F(\alpha_1, \ldots \alpha_n)$

Proof: ($\Rightarrow$) If $[K:F]=n$. Let $\alpha_1, \dots \alpha_n$ be a basis of K over F. $F \subset F(\alpha_i) \subset K$

Then $[F(\alpha_i):F] \mid [K:F]$ and is finite

hence each α_i is algebraic over F

K is obviously generated by α_i over F.

($\Leftarrow$) The converse is also easy. Since α_i's are algebraic over F, they are also alg over any extention of F. We have a tower of fields

$$[K:F] = [F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) : F(\alpha_1, \dots \alpha_{n-1})]$$

$$\times [F(\alpha_1, \dots \alpha_{n-2})(\alpha_{n-1}) : F(\alpha_1, \dots \alpha_{n-2})]$$

$$\vdots$$

$$\times [F(\alpha_1)(\alpha_2) : F(\alpha_1)]$$

$$\times [F(\alpha_1) : F]$$

Hence each degree is finite on the RHS, the LHS ie $[K:F]$ is also finite $\blacksquare$

Thm 2.15. If L is algebraic over K, and K is algebraic over F then L is algebraic over F.

Pf. Exercise (Sheet 4)

Finally we have the following useful Proposition

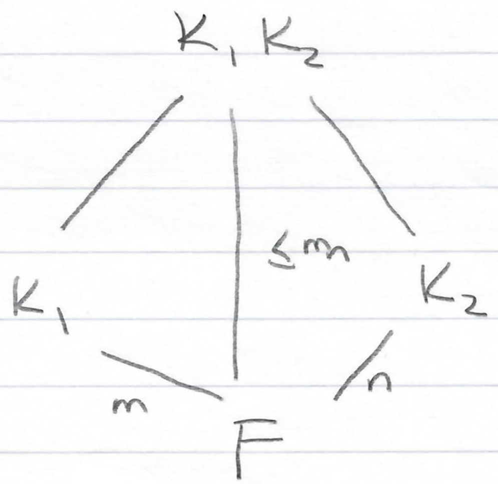
Prop 2-16 let $F \subset K_1, K_2 \subset K$ with K_1, K_2 2 finite extensions of F. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

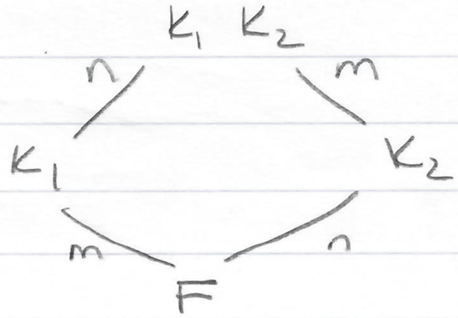
Proof Exercise serie 2

Cor 2-17 Suppose $[K_1 : F] = m$, $[K_2 : F] = n$ and $\gcd(m,n) = 1$. Then

$$[K_1K_2 : F] = [K_1 : F][K_2 : F] = mn.$$



If $(m,n) = 1$ then



<u>Example</u> $K = \mathbb{Q}(\sqrt[6]{2}, \sqrt{2})$

Note $\sqrt{2} \in \mathbb{Q}(\sqrt[6]{2})$, Since

$\sqrt{2} = (\sqrt[6]{2})^3 \in \mathbb{Q}(\sqrt[6]{2})$. Hence

$\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$. Hence

$\mathbb{Q}(\sqrt[6]{2}, \sqrt{2}) = \mathbb{Q}(\sqrt[6]{2})$ and

$[\mathbb{Q}(\sqrt[6]{2}, \sqrt{2}) : \mathbb{Q}(\sqrt[6]{2})] = 1$

$\sqrt[6]{2}$ is a zero of $x^6 - 2 \in \mathbb{Q}[x]$ which is irred. by Eisenstein.

Hence $m_{\sqrt[6]{2}, \mathbb{Q}}(x) = x^6 - 2$ and

$[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$. We have the tower of fields

$$
\begin{tikzcd}
 & \mathbb{Q}(\sqrt[6]{2}, \sqrt{2}) = \mathbb{Q}(\sqrt[6]{2}) \arrow[dl, dash] \arrow[dd, dash, "6"] \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \\
 & \mathbb{Q}
\end{tikzcd}
$$

Hence by tower rule $[\mathbb{Q}(\sqrt[6]{2}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 3$
Hence the min. poly of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$ has degree 3. Since $(\sqrt[6]{2})^3 = \sqrt{2}$
$\sqrt[6]{2}$ satisfies $x^3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$ which also has degree 3. Since it is also monic

$x^3 - \sqrt{2}$ must be the min-poly of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$.

(Showing $x^3 - \sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt{2})$ directly is not trivial.)

<u>Example</u> $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = ?$

$$
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{3}, \sqrt{5}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

By Prop 2.15 $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] \leq [\mathbb{Q}\sqrt{3} : \mathbb{Q}][\mathbb{Q}\sqrt{5} : \mathbb{Q}]$
≤ 4

Since $(\sqrt{5})^2 = 5 \in \mathbb{Q} \subset \mathbb{Q}(\sqrt{3})(\sqrt{5})$

$\sqrt{5}$ has degree at most 2 over $\mathbb{Q}(\sqrt{3})$

It has degree $1 \Leftrightarrow \sqrt{5} \in \mathbb{Q}(\sqrt{3})$. Suppose

$\sqrt{5} = a + b\sqrt{3}$ with $a, b \in \mathbb{Q}$. Then

$5 = a^2 + 3b^2 + 2ab\sqrt{3}$

$\Rightarrow \dfrac{5 - a^2 - 3b^2}{2ab} = \sqrt{3} \Rightarrow \sqrt{3}$ is rational ↯

Hence $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$ and $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$.