Math 5402

4/6/20

week 11

Test 2

Scheduled for 4/15
Move to 4/22

13.2 – continued...

Def: Let F be a field and α be algebaic over F. The unique irreducible and monic polynomial in $F[x]$ having α as a root will be denoted by $m_{\alpha,F}(x)$ and is called the minimal polynomial for α over F. The degree of $m_{\alpha,F}(x)$ is sometimes called the degree of α over F.

Ex: $\alpha = 2^{1/n}$

$F = \mathbb{Q}$

$f(x) = x^n - 2$

- $x^n - 2 \in \mathbb{Q}[x]$
- $f(2^{1/n}) = 0$
- $x^n - 2$ is monic
- Using Eisenstein w/ $p = 2$ gives that $x^n - 2$ is irreducible over $\mathbb{Q}$.

So, $m_{2^{1/n}, \mathbb{Q}}(x) = x^n - 2$

Thm: Let α be algebraic over a field F. Then,

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

So,

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

Ex: $m_{2^{1/n},\mathbb{Q}}(x) = x^n - 2$

$$[\mathbb{Q}(2^{1/n}) : \mathbb{Q}] = \deg(x^n - 2) = n$$

basis of $\mathbb{Q}(2^{1/n})$ over $\mathbb{Q}$ $= \{1, 2^{1/n}, (2^{1/n})^2, \ldots, (2^{1/n})^{n-1}\}$

$$\mathbb{Q}(2^{1/n}) = \left\{ a_0 + a_1 2^{1/n} + a_2 (2^{1/n})^2 + \ldots + a_{n-1} (2^{1/n})^{n-1} \;\middle|\; a_i \in \mathbb{Q} \right\}$$

$$= \left\{ a_0 + a_1 2^{1/n} + a_2 2^{2/n} + \ldots + a_{n-1} 2^{(n-1)/n} \;\middle|\; a_i \in \mathbb{Q} \right\}$$

Vector space theorem

Let F, K, L be fields with $F \subseteq K \subseteq L$.

Then,

$$[L:F] = [L:K][K:F]$$

(if these #s are finite)

(proof is Thm 14 in the book)

proof (sketchy):

Let $\{\beta_1, \beta_2, \dots, \beta_n\}$ is a basis for K over F and $\{\gamma_1, \gamma_2, \dots, \gamma_m\}$ is a basis for L over K. Then

$$\left\{ \beta_i \gamma_j \;\middle|\; \begin{array}{l} 1 \leq i \leq n \\ 1 \leq j \leq m \end{array} \right\} = \{\beta_1\gamma_1, \beta_2\gamma_1, \dots, \beta_n\gamma_1, \beta_1\gamma_2, \beta_2\gamma_2, \dots, \beta_n\gamma_2, \dots, \beta_1\gamma_m, \beta_2\gamma_m, \dots, \beta_n\gamma_m\}$$

is a basis for L over F. ∎

Ex: $[\mathbb{Q}(2^{1/6}):\mathbb{Q}] = 6$

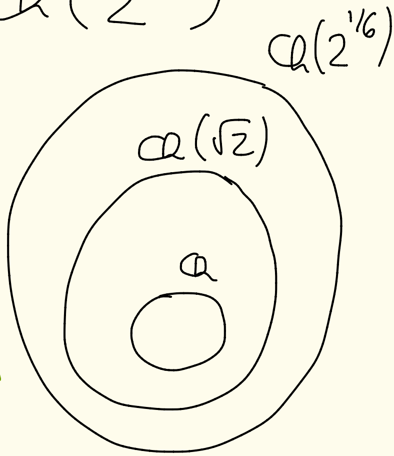
$m_{2^{1/6},\mathbb{Q}}(x) = x^6 - 2$

Is $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(2^{1/6})$?

Yes! $\sqrt{2} = (2^{1/6})^3 \in \mathbb{Q}(2^{1/6})$

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

$\boxed{m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2}$



By previous theorem,

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

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

$$\begin{tikzcd}
\mathbb{Q}(2^{1/6}) \arrow[d, dash, "3"] \arrow[dd, dash, bend right=60, "6"'] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

$3 \leftarrow m_{2^{1/6}, \mathbb{Q}(\sqrt{2})}(x) = x^3 - \sqrt{2}$

$2 \leftarrow m_{\sqrt{2}, \mathbb{Q}}(x) = x^2 - 2$

Note $x^3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

$2^{1/6}$ is a root of $x^3 - \sqrt{2}$.

Note that $(\mathbb{Q}(\sqrt{2}))(2^{1/6}) =$

$= \mathbb{Q}(\sqrt{2}, 2^{1/6}) \underset{\boxed{\sqrt{2} \in \mathbb{Q}(2^{1/6})}}{=} \mathbb{Q}(2^{1/6})$

$\boxed{\text{Next page we will show } F(\alpha, \beta) = (F(\alpha))(\beta)}$

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

$= [(\mathbb{Q}(\sqrt{2}))(2^{1/6}) : \mathbb{Q}(\sqrt{2})] = \deg(m_{2^{1/6}, \mathbb{Q}(\sqrt{2})}(x))$

So, $\min_{2^{1/6}, \mathbb{Q}(\sqrt{2})}(x) = x^3 - \sqrt{2}$

Thm: $F(\alpha, \beta) = (F(\alpha))(\beta)$

(Lemma 16 in the book)

Ex: Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$

$\Big|\ n$

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

$\Big|\ 2 \leftarrow m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$

$\mathbb{Q}$

What is n?

Note that $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$.

And $\sqrt{3}$ is a root of $x^2 - 3$. Let's show that $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,/\, a, b \in \mathbb{Q}\}$

Since $x^2 - 3$ has degree 2, we can just show it has no roots in $\mathbb{Q}(\sqrt{2})$ and thus its irreducible over $\mathbb{Q}(\sqrt{2})$. The roots of $x^2 - 3$ are $\pm\sqrt{3}$. Suppose $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$.

Then, $\sqrt{3} = a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$.

If $b = 0$, then $\sqrt{3} = a \in \mathbb{Q}$ which isn't the case.

If $a = 0$, then $\sqrt{\frac{3}{2}} = \frac{\sqrt{3}}{\sqrt{2}} = b \in \mathbb{Q}$ which isn't the case.

If $a \neq 0$ and $b \neq 0$, then squaring both sides gives $(\sqrt{3})^2 = (a + b\sqrt{2})^2$ which is

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

Then, $\sqrt{2} = \dfrac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}$

which can't happen.

Thus, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

So, $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$ and thus $m_{\sqrt{3}, \mathbb{Q}(\sqrt{2})}(x) = x^2 - 3$.

So,

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ \big| \; 2 = n \\ \mathbb{Q}(\sqrt{2}) \end{array} \qquad \boxed{m_{\sqrt{3}, \mathbb{Q}(\sqrt{2})}(x) = x^2 - 3}$$

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[d, dash, "2"] \arrow[dd, dash, bend right, "4"'] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ is $\{1, \sqrt{3}\}$

basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}\}$

So a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$ is $\{1, 1\cdot\sqrt{3}, \sqrt{2}\cdot 1, \sqrt{2}\cdot\sqrt{3}\}$ which is $\{1, \sqrt{3}, \sqrt{2}, \sqrt{6}\}$.

So, $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$ and

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a + b\sqrt{3} + c\sqrt{2} + d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\}$$