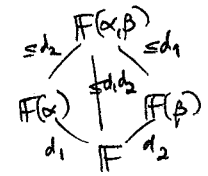
(63)
3/13/2019

§15.4 Computing $m_{\mathbb{F},\alpha}(x)$

Since $m_{\mathbb{F},\alpha}(x) = a_0 + a_1 x + \ldots + a_n x^n$ is an $\mathbb{F}$-linear dependence on $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$, when looking for it, this can help:



(LEMMA: (15.4.2)) If $\gamma \in \mathbb{F}(\alpha,\beta)$ with $[\mathbb{F}(\alpha):\mathbb{F}] = d_1$, $[\mathbb{F}(\beta):\mathbb{F}] = d_2$

then since $\{\alpha^i \beta^j\}_{\substack{0 \leq i \leq d_1 \\ 0 \leq j \leq d_2}}$ $\mathbb{F}$-span $\mathbb{F}(\alpha,\beta)$ (and give an $\mathbb{F}$-basis when $[\mathbb{F}(\alpha,\beta):\mathbb{F}] = d_1 d_2$)

there must exist a dependence $a_0 + a_1\gamma + a_2\gamma^2 + \ldots + a_{d_1 d_2}\gamma^{d_1 d_2} = 0$ with $a_i \in \mathbb{F}$

i.e. $\deg m_{\mathbb{F},\gamma}(x) \leq d_1 d_2$

proof: We saw the spanning argument already in proving multiplicativity $[\mathbb{L}:\mathbb{F}] = [\mathbb{L}:\mathbb{K}][\mathbb{K}:\mathbb{F}]$ ∎

EXAMPLE: Quadratic fields $= \mathbb{Q}(\sqrt{a})$
Biquadratic fields $= \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b \in \mathbb{Q}$

e.g. $\mathbb{Q}\left(\sqrt{\frac{5}{8}}\right) = \mathbb{Q}\left(8\sqrt{\frac{5}{8}}\right) = \mathbb{Q}\left(\sqrt{5\cdot 8}\right) = \mathbb{Q}\left(2\sqrt{2\cdot 5}\right) = \mathbb{Q}\left(\sqrt{2\cdot 5}\right) = \mathbb{Q}\left(\sqrt{10}\right)$

WLOG $a \in \mathbb{Z}$ and is square-free

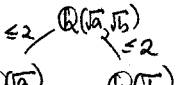
$\mathbb{Q}\left(\sqrt{22}, \sqrt{-1400}\right) = \mathbb{Q}\left(\sqrt{22}, \sqrt{-14}\right)$

$= \mathbb{Q}\left(\sqrt{2\cdot 11}, \sqrt{-2\cdot 7}\right)$

WLOG $a, b \in \mathbb{Z}$ both squarefree and not the same list of prime factors (unless its $\mathbb{Q}(\sqrt{a}, \sqrt{-a}) = \mathbb{Q}(i, \sqrt{a})$, $\sqrt{-1} = 11$)

PROPOSITION: For $a, b \in \mathbb{Z}$ squarefree with not same prime factors,

$[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}] = 4$ with $\mathbb{Q}$-basis $\{1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\}$

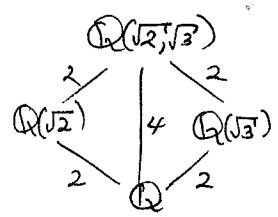
proof: 

Only need $\sqrt{b} \notin \mathbb{Q}(\sqrt{a})$ i.e. $\sqrt{b} = r + s\sqrt{a}$ with $r, s \in \mathbb{Q}$

$\Rightarrow b = r^2 + 2rs\sqrt{a} + s^2 a \Rightarrow rs = 0 \Rightarrow r = 0$ or $s = 0$

$\sqrt{b} = s\sqrt{a}$, $b = s^2 a$ Contradiction

$\sqrt{b} = r$, $b = r^2$ Contradiction ∎



e.g. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ has $\mathbb{Q}$-basis $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$

and hence $\gamma=\sqrt{2}+\sqrt{3}$ has $\deg(m_{\mathbb{Q},\gamma}(x))\le 4$.

Write $1,\gamma,\gamma^2,\gamma^3,\gamma^4$ in the above $\mathbb{Q}$-basis to find it:

$$\left.\begin{aligned} 1 &= 1 \\ \gamma &= \sqrt{2}+\sqrt{3} \\ \gamma^2 &= 5 + 2\sqrt{6} \\ \gamma^3 &= 11\sqrt{2}+9\sqrt{3} \\ \gamma^4 &= 49 + 20\sqrt{6} \end{aligned}\right\} \Rightarrow \gamma^4 = 10\gamma^2 - 1$$

$$\gamma^4 - 10\gamma^2 + 1 = 0$$

so $m_{\mathbb{Q},\gamma}(x)$ is a <u>factor</u> of x^4-10x^2+1,

but we must have $m_{\mathbb{Q},\gamma}(x)=x^4-10x^2+1$

since $\{1,\gamma,\gamma^2,\gamma^3\}$ are $\mathbb{Q}$-linearly independent by <u>inspection</u>;

actually only need to check $\{1,\gamma,\gamma^2\}$ are independent since

$[\mathbb{Q}(\gamma):\mathbb{Q}]=3$ is impossible (Why?).

Artin (anticipating Chap. 16) suggests guessing the <u>roots</u> of $m_{\mathbb{Q},\gamma}(x)$,

besides $\gamma=\sqrt{2}+\sqrt{3}$, might be $\pm\sqrt{2}\pm\sqrt{3}$

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

so guess $(x-(\sqrt{2}+\sqrt{3}))(x+(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))$

$$= (x^2-(\sqrt{2}+\sqrt{3})^2)(x^2-(\sqrt{2}-\sqrt{3})^2)$$

some algebra! $= x^4-10x+1$

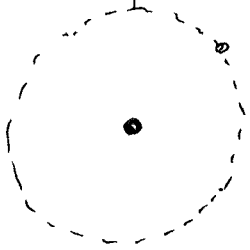
§15.5 Compass & straightedge constructions

We'll show impossibility of three constructions by understanding where distances between points lie in $\mathbb{R}$, as a subfield of $\mathbb{R}$...

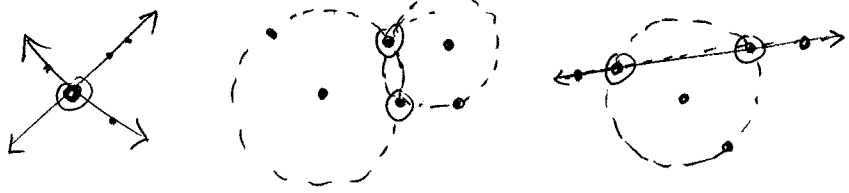
DEF'N: Starting with two initial constructed points $(0,0), (1,0)$ in $\mathbb{R}^2$, call constructible lines, circles, points all those obtained by iterating these operations:

(a) draw a new constructible line through two constructed points:

(b) draw a new constructible circle with center on one constructed point and passing through a second such point:



(c) create new constructed points as intersections of two constructed lines or circles or circle & line



DEF'N: Any $\alpha \in \mathbb{R}$ that is a distance $\alpha = \|p - p'\|$ between two constructible points $p, p' \in \mathbb{R}^2$ is called a constructible distance

Let $\mathbb{K}_{con} := \{\text{all constructible distances } \alpha \in \mathbb{R}\}$