3/6/2019 >
(55)

proof of PROP-DEF'N:

(a): Assume α is algebraic over $\mathbb{F}$, so $\ker\left(\mathbb{F}[x] \xrightarrow{\varphi} \mathbb{K}\right) \overset{\mathbb{F}[x] \text{ is a PID}}{=} (f(x))$
$x \longmapsto \alpha$

for some unique monic polynomial $f(x)$, namely the monic polynomial in $\ker(\varphi)$ of minimum degree.

We claim this $f(x)$ is irreducible since if $f(x)=g(x)h(x)$ properly
then $0=f(\alpha)=g(\alpha)h(\alpha)$
forces either $g(\alpha)=0$ or $h(\alpha)=0$ since $\mathbb{F}$ is a domain; contradiction to minimum degree for f.

Conversely if some irreducible monic $g(x) \in \mathbb{F}[x]$ lies in $\ker(\varphi)=(f(x))$

then $f | g \underset{g \text{ is irreducible}}{\Rightarrow} f,g$ associate $\underset{f,g \text{ monic}}{\Rightarrow} f=g$.

Noether's 1st implies $\mathbb{F}[x]/(f(x)) \cong \mathrm{im}\varphi = \mathbb{F}[\alpha] \overset{\text{subring}}{\subset} \mathbb{K}$,

but then f irred. $\Rightarrow (f(x))$ maximal $\Rightarrow \mathbb{F}[x]/(f(x))$ is a field

$\Rightarrow \mathbb{F}[\alpha]$ is a field, a subfield of $\mathbb{K}$

$\Rightarrow \mathbb{F}[\alpha] \subseteq \mathbb{F}(\alpha)$ must actually be an equality: $\mathbb{F}[\alpha]=\mathbb{F}(\alpha)$

smallest subfield of $\mathbb{K}$ containing $\mathbb{F},\alpha$

We also know $\mathbb{F}[x]/(f(x)) \longleftarrow \mathbb{F}^n$ is an $\mathbb{F}$-vector space iso.,

$c_0+c_1\bar{x}+\dots+c_{n-1}\bar{x}^{n-1} \longleftarrow\!\shortmid \begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix}$

i.e. $\{\bar{1},\bar{x},\bar{x}^2,\dots,\bar{x}^{n-1}\}$ is an $\mathbb{F}$-basis for $\mathbb{F}[x]/f(x)$,

so $\{1,\alpha,\alpha^2,\dots,\alpha^{n-1}\}$ is an $\mathbb{F}$-basis for $\mathbb{F}[\alpha]=\mathbb{F}(\alpha)$.

(b): If α is transcendental then $\ker\left(\mathbb{F}[x] \xrightarrow{\varphi} \mathbb{K}\right) = \{0\}$
$x \longmapsto \alpha$

so Noether's 1st implies $\mathbb{F}[x] \cong \mathrm{im}\varphi = \mathbb{F}[\alpha] \overset{\text{subring}}{\subset} \mathbb{K}$

Then $\mathbb{F}(\alpha) \cong \mathrm{Frac}(\mathbb{F}[\alpha]) \cong \mathrm{Frac}(\mathbb{F}[x]) = \mathbb{F}(x)$

It's not always obvious that two descriptions $\mathbb{F}[x]/(f_1(x))$, $\mathbb{F}[x]/(f_2(x))$ might be isomorphic to the same extension $\mathbb{F}[\alpha] \subset \mathbb{K}$

EXAMPLE: $\alpha := \sqrt{2}+1 \in \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$

and $\underset{\alpha-1}{\underset{\parallel}{\sqrt{2}}} \in \mathbb{Q}[\alpha] \subset \mathbb{R}$, so $\mathbb{Q}[\sqrt{2}+1] = \mathbb{Q}[\sqrt{2}]$

But α has different irreducible polynomial over $\mathbb{Q}$ than $\sqrt{2}$, which has $m_{\mathbb{Q},\sqrt{2}}(x) = x^2-2$:

$$\alpha^2 = (\sqrt{2}+1)^2 = 2+2\sqrt{2}+1 = 3+2\sqrt{2} = 3+2(\alpha-1) = 3+2\alpha-2 = 1+2\alpha$$

$$\Rightarrow \alpha^2-2\alpha-1=0$$

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

because it is irreducible (over $\mathbb{Q}$) by rational root test

Hence $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[\sqrt{2}] = \mathbb{Q}[\sqrt{2}+1] \cong \mathbb{Q}[x]/(x^2-2x-1)$

Not obviously isomorphic!

And sometimes two extensions $\mathbb{F}(\alpha), \mathbb{F}(\beta) \subset \mathbb{K}$ are not equal $\mathbb{F}[\alpha_1] \neq \mathbb{F}[\alpha_2]$,

but there is an F-isomorphism of the extensions

$$\begin{array}{ccc} \mathbb{F} & \subset & \mathbb{F}(\alpha) \\ & & \downarrow \varphi \\ \mathbb{F} & \subset & \mathbb{F}(\beta) \end{array}$$

DEF'N (15.29): Say $\mathbb{F} \begin{smallmatrix} \subset \mathbb{K} \\ \subset \mathbb{K}' \end{smallmatrix}$ two field extensions of $\mathbb{F}$ are $\mathbb{F}$-isomorphic

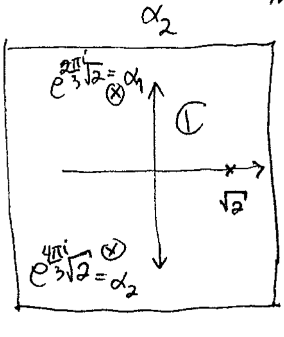
if $\exists$ a field isomorphism $\mathbb{K} \xrightarrow{\varphi} \mathbb{K}'$ with $\varphi|_{\mathbb{F}} = 1_{\mathbb{F}}$

"φ restricted to $\mathbb{F}$" (the identity map on $\mathbb{F}$)

i.e. $\varphi(c) = c \ \forall c \in \mathbb{F}$

EXAMPLES: ① $+i, -i \in \mathbb{C}$ are both roots of $x^2+1 \in \mathbb{Q}[x] \subset \mathbb{R}[x]$, and $\exists$ an $\mathbb{R}$-isomorphism / $\mathbb{Q}$-isomorphism $\begin{matrix} \mathbb{C} \xrightarrow{\varphi} \mathbb{C} \\ z \mapsto \bar{z} \end{matrix}$ sending $+i \mapsto -i$

② $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(\underset{m_{\mathbb{Q},\sqrt[3]{2}}(x)}{\underset{\parallel}{x^3-2}})$, but $\underset{\alpha_1}{\underset{\parallel}{e^{\frac{2\pi i}{3}}\sqrt[3]{2}}}$ and $\underset{\alpha_2}{\underset{\parallel}{e^{\frac{4\pi i}{3}}\sqrt[3]{2}}}$ also have $m_{\mathbb{Q},\alpha_1}(x) = m_{\mathbb{Q},\alpha_2}(x) = x^3-2$ (why?)



Hence there are $\mathbb{Q}$-isomorphisms that send $\sqrt[3]{2} \mapsto e^{\frac{2\pi i}{3}}\sqrt[3]{2} \mapsto e^{\frac{4\pi i}{3}}\sqrt[3]{2}$

coming from $\mathbb{Q}(\sqrt[3]{2})^{\subset \mathbb{R}} \cong \mathbb{Q}(e^{\frac{2\pi i}{3}}\sqrt[3]{2})^{\subset \mathbb{C}} \cong \mathbb{Q}(e^{\frac{4\pi i}{3}}\sqrt[3]{2})$

$$\begin{array}{ccccc} \mathbb{Q}(\sqrt[3]{2}) & & \mathbb{Q}(e^{\frac{2\pi i}{3}}\sqrt[3]{2}) & & \mathbb{Q}(e^{\frac{4\pi i}{3}}\sqrt[3]{2}) \\ & \nwarrow \cong & \Big\| \wr & \cong \nearrow & \\ & & \mathbb{Q}[x]/(x^2-2) & & \end{array}$$

$\sqrt[3]{2} \leftarrow\!\shortmid x$, $\quad e^{\frac{2\pi i}{3}}\sqrt[3]{2} \leftarrow\!\shortmid x$, $\quad x \mapsto e^{\frac{4\pi i}{3}}\sqrt[3]{2}$

(57)

PROPOSITION: (15.2.10) Given two extensions $\mathbb{F} \begin{smallmatrix} \subset \mathbb{K} \\ \subset \mathbb{K}' \end{smallmatrix}$ and $\alpha \in \mathbb{K}$, $\alpha' \in \mathbb{K}'$,

(a) if there is an $\mathbb{F}$-isomorphism $\mathbb{K} \xrightarrow{\varphi} \mathbb{K}'$ sending $\alpha \longmapsto \alpha'$ then $m_{\mathbb{F},\alpha}(x) = m_{\mathbb{F},\alpha'}(x)$ $\left(\in \mathbb{F}[x]\right)$

(b) conversely if $m_{\mathbb{F},\alpha}(x) = m_{\mathbb{F},\alpha'}(x)$ then there is at least an $\mathbb{F}$-isomorphism

$$\begin{array}{ccc} \mathbb{F}(\alpha) & \xrightarrow{\varphi} & \mathbb{F}(\alpha') \\ \cap & & \cap \\ \mathbb{K} & & \mathbb{K}' \end{array}$$

Proof: For (a), since $m_{\mathbb{F},\alpha}(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{F}[x]$, $a_i \in \mathbb{F}$

has $0 = m_{\mathbb{F},\alpha}(\alpha) = a_0 + a_1\alpha + \dots + a_n\alpha^n$ in $\mathbb{K}$

apply φ, (fixing all a_i, sending $\alpha \mapsto \alpha'$) $\downarrow$

$$0 = \varphi(0) = a_0 + a_1\alpha' + a_1(\alpha')^2 + \dots + a_n(\alpha')^n = m_{\mathbb{F},\alpha}(\alpha') \text{ in } \mathbb{K}'$$

$$\Longrightarrow \underbrace{m_{\mathbb{F},\alpha}(x)}_{\text{irred. in } \mathbb{F}[x]} = m_{\mathbb{F},\alpha'}(x).$$

For (b), if $m_{\mathbb{F},\alpha}(x) = m_{\mathbb{F},\alpha'}(x)$ then

$$\begin{array}{ccccc} \mathbb{K} & & & & \mathbb{K}' \\ \cup & & & & \cup \\ \mathbb{F}(\alpha) & \overset{\varphi_1}{\cong} & \mathbb{F}[x]/(m_{\mathbb{F},\alpha}(x)) & \overset{\varphi_2}{\cong} & \mathbb{F}(\alpha') \\ & & \text{''} & & \\ & & m_{\mathbb{F},\alpha'}(x) & & \\ \alpha & \longleftarrow & x & & \\ & & x & \longmapsto & \alpha' \end{array}$$

so $\varphi = \varphi_2 \circ \varphi_1 : \mathbb{F}(\alpha) \longrightarrow \mathbb{F}(\alpha')$ is the desired $\mathbb{F}$-isomorphism ■
$\qquad \alpha \longmapsto \alpha'$