3.3 Tutorial 1 NEW MAST30005 Semester 1, 2024: Last week's theorems

Last week we covered the following theorems. Write careful proofs of each.

Proposition 3.1. *Let $\mathbb{K}$ be a field and let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$. Then $\mathbb{K}^H$ is a subfield of $\mathbb{K}$.*

Theorem 3.2. *Let $\varphi\colon A \to R$ be a ring homomorphism. Let $K = \ker(\varphi)$. Then the function*

$$\begin{array}{ccc} \dfrac{A}{\ker(\varphi)} & \to & \mathrm{im}(\varphi) \\ a+K & \mapsto & \varphi(a) \end{array} \qquad \textit{is a ring isomorphism.}$$

Proposition 3.3. *Let $\mathbb{F}$ be a subfield of a field $\mathbb{K}$ and let $\alpha \in \mathbb{K}$. Let $\mathbb{F}[x] \overset{\mathrm{ev}_\alpha}{\to} \mathbb{K}$ be the evaluation homomorphism. Let $\mathbb{F}(\alpha)$ be the smallest subfield of $\mathbb{K}$ containing $\mathbb{F}$ and α. Let*

$$\mathbb{F}[\alpha] = \mathrm{im}(\mathrm{ev}_\alpha) \qquad \textit{and let} \quad m_{\alpha,\mathbb{F}}(x) = c_0 + c_1 x + \cdots c_{\ell-1}x^{\ell-1} + x^\ell \quad \in \mathbb{F}[x]$$

be such that

$$\ker(\mathrm{ev}_\alpha) = (m_{\alpha,\mathbb{F}}(x)), \qquad \textit{where} \quad (m_{\alpha,\mathbb{F}}(x)) = m_{\alpha,\mathbb{F}}(x)\mathbb{F}[x] = \{m_{\alpha,\mathbb{F}}(x)g \mid g \in \mathbb{F}[x]\}.$$

Then

$$\mathbb{F}(\alpha) = \mathbb{F}[\alpha] \cong \frac{\mathbb{F}[x]}{(m_{\alpha,\mathbb{F}}(x))},$$

and, as a vector space over $\mathbb{F}$,

$$\mathbb{F}(\alpha) \qquad \textit{has } \mathbb{F}\textit{-basis} \quad \{1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}\}.$$

Theorem 3.4. *Let $\mathbb{E}$ be a subfield of $\mathbb{K}$ and assume that there exists $f \in \mathbb{E}[x]$ such that $\mathbb{K}$ is the splitting field of f over $\mathbb{E}$. Then the map*

$$\begin{array}{ccc} \{\textit{field inclusions } \mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}\} & \longleftrightarrow & \{\textit{group inclusions } \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \supseteq H \supseteq \{1\}\} \\ \mathbb{F} & \longmapsto & \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \\ \mathbb{K}^H & \longleftarrow & H \end{array}$$

is an isomorphism of posets.

Some steps for the proof of Theorem 3.4:

Let $\mathbb{K}$ be a field.

- Let $\mathbb{F}$ be a subfield of $\mathbb{K}$. The **Galois group of $\mathbb{K}$ over $\mathbb{F}$** is

$$\mathrm{Gal}(\mathbb{F}) = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) = \{\sigma \in \mathrm{Aut}(\mathbb{K}) \mid \text{if } e \in \mathbb{F} \text{ then } \sigma(e) = e\}.$$

- Let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$. The **fixed field of H** is

$$\mathrm{Fix}(H) = \mathbb{K}^H = \{e \in \mathbb{K} \mid \text{if } \sigma \in H \text{ then } \sigma(e) = e\}.$$

HW: Show that $\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$ is a subgroup of $\mathrm{Aut}(\mathbb{K})$.

HW: Show that $\mathbb{K}^H$ is a subfield of $\mathbb{K}$.

HW: Let $\mathbb{F} \subseteq \mathbb{K}$ be a subfield of $\mathbb{K}$. Show that $\mathrm{Fix}(\mathrm{Gal}(\mathbb{F}) \supseteq \mathbb{F}$.

HW: Let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$. Show that $\mathrm{Gal}(\mathrm{Fix}(H)) \subseteq H$.

HW: Let $\mathbb{F}$ and $\mathbb{G}$ be subfields of $\mathbb{K}$ and assume that $\mathbb{F} \subseteq \mathbb{G}$. Show that $\mathrm{Gal}(\mathbb{G}) \subseteq \mathrm{Gal}(\mathbb{F})$.

HW:. Let G and H be subgroups of $\mathrm{Aut}(\mathbb{K}))$ and assume that $G \subseteq H$. Show that $\mathrm{Fix}(G) \supseteq \mathrm{Fix}(H)$.

HW:. Let H be a subgroup of $\mathrm{Aut}(\mathbb{K}))$. Show that $\mathrm{Fix}(\mathrm{Gal}(\mathrm{Fix}(H))) = \mathrm{Fix}(H)$.

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$. Show that $\mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(\mathbb{F}))) = \mathrm{Gal}(\mathbb{F})$.

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and let $\sigma \in \mathrm{Aut}(\mathbb{E})$. Show that $\mathrm{Gal}(\sigma(\mathbb{F})) = \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$ (subgroups of $\mathrm{Aut}(\mathbb{K})$).

HW:. Let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$ and let $\sigma \in \mathrm{Aut}(\mathbb{E})$. Show that $\mathrm{Fix}(\sigma H \sigma^{-1}) = \sigma(\mathrm{Fix}(H))$ (subfields of $\mathbb{K}$).

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is the splitting field of a polynomial $f(x) \in \mathbb{F}[x]$ over $\mathbb{F}$ and that $f(x)$ factors as

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_\ell), \qquad \text{with } \alpha_1, \ldots, \alpha_\ell \in \mathbb{K}.$$

Show that $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_\ell)$.

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_\ell)$. Show that there exists $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$.

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Show that there exists $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$.

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Let $\gamma \in \mathbb{K}$ such that $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$. Let $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Show that

$$m_{\gamma,\mathbb{F}}(x) = \prod_{\beta \in G\gamma} (x - \beta).$$

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Let $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$. Let $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Show that

$$\deg(m_{\gamma,\mathbb{F}}(x)) = |G|.$$

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Let $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$. Let $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Show that

$$\dim_{\mathbb{F}}(\mathbb{K}) = |G|.$$

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Let $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$. Let $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Let $G\gamma = \{g\gamma \mid g \in G\}$. Show that

$$\begin{array}{ccc} G & \to & G\gamma \\ g & \mapsto & g\gamma \end{array}$$

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Let $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$. Show that $\mathrm{Fix}(\mathrm{Gal}(\mathbb{F})) = \mathbb{F}$.

HW:. Let H be a finite subgroup of $\mathrm{Aut}(\mathbb{K})$. Show that $\mathbb{K} \supseteq \mathbb{K}^H$ is a Galois extension.

HW:. Let H be a finite subgroup of $\mathrm{Aut}(\mathbb{K})$. Show that $\mathrm{Gal}(\mathrm{Fix}(H)) = H$.